GFI Product Manual

GFI EndPointSecurity™

Administrator Guide

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, frequency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.

All product and company names herein may be trademarks of their respective owners.

GFI EndPointSecurity is copyright of GFI SOFTWARE Ltd. - 1999-2013 GFI Software Ltd. All rights reserved.

Document Version: 1.1.1

Last updated (month/day/year): 25/03/2013

Contents

1 Introduction **11**

1.0.1 Terms and conventions used in this guide 11
1.1 Portable media device threats 11
1.2 About GFI EndPointSecurity 12
1.3 Components of GFI EndPointSecurity 12
1.3.1 GFI EndPointSecurity Management Console 13
1.3.2 GFI EndPointSecurity Agent 13
1.4 Key Features 13
1.5 How GFI EndPointSecurity works - Deployment and Monitoring 14
1.6 How GFI EndPointSecurity works - Device Access 16
1.7 How GFI EndPointSecurityworks - Temporary Access 17
1.8 Supported device categories 18
1.9 Supported connectivity ports 19
1.10 Navigating the Management Console 19

2 Installing GFI EndPointSecurity **21**

2.1 System requirements 21
2.2 Upgrading GFI EndPointSecurity 22
2.3 Installing a new instance of GFI EndPointSecurity 23
2.4 Post-install configurations 25
2.5 Navigating the Management Console 27
2.6 Testing your installation 29
2.6.1 Test preconditions 29
2.6.2 Test case 30
2.6.3 Reverting to default settings 33

3 Achieving Results **34**

3.1 Preventing data leaks and malware infections 34
3.2 Automating network protection 35
3.3 Monitoring network activity from a central location 37

4 Adding Target Computers **38**

4.1 Adding computers manually 38
4.2 Adding computers automatically 39
4.3 Configuring log on credentials 42

5 Managing Protection Policies **45**

5.1 Creating a new protection policy 45
5.2 Assigning a Protection Policy 51
5.2.1 Deploy immediately 52
5.2.2 Scheduled policy deployment 53
5.2.3 Deploying policies through Active Directory 54
5.3 Verifying protection policy deployment 54
5.3.1 Deployment History 55
5.3.2 Agents' status 55

6 Customizing Protection Policies **57**
6.1 Configuring controlled device categories 57
6.2 Configuring controlled connectivity ports 58
6.3 Configuring power users 59
6.4 Configuring access permissions for device categories 60
6.5 Configuring access permissions for connectivity ports 63
6.6 Configuring access permissions for specific devices 65
6.7 Viewing access permissions 68
6.8 Configuring priorities for permissions 70
6.9 Configuring device blacklist 70
6.10 Configuring device whitelist 74
6.11 Configuring temporary access privileges 77
6.11.1 Requesting temporary access for a protected computer 77
6.11.2 Granting temporary access to a protected computer 79
6.12 Configuring file-type filters 81
6.13 Configuring content awareness 83
6.13.1 Managing content awareness options 83
6.13.2 Managing template options 85
6.14 Configuring file options 86
6.15 Configuring security encryption 88
6.15.1 Configuring Microsoft BitLocker To Go devices 88
6.15.2 Configuring Volume Encryption 90
6.16 Configuring event logging 94
6.17 Configuring alerts 96
6.18 Setting a policy as the default policy 99

7 Discovering Devices **100**
7.1 Running a device scan 100
7.2 Analyzing device scan results 103
7.2.1 Computers 104
7.2.2 Devices list 104
7.3 Adding discovered devices to the database 104

8 Monitoring Device Usage Activity **106**
8.1 Statistics 106
8.1.1 Protection Status 107
8.1.2 Device Usage by Device Type 107
8.1.3 Device Usage by Connectivity Port 108
8.2 Activity 108
8.2.1 Activity Log 108
8.2.2 Advanced Filtering 109
8.2.3 Logs Browser 110
8.2.4 Creating event queries 111

9 Status Monitoring **113**
9.1 Risk Assessment view 113
9.2 Statistics view 115

9.2.1 Protection Status ... 116
9.2.2 Device Usage by Device Type ... 117
9.2.3 Device Usage by Connectivity Port ... 117
9.3 Status view ... 117
9.4 Deployment status view ... 119
9.4.1 About Deployment status view ... 120
9.4.2 Current Deployments ... 121
9.4.3 Queued Deployments ... 121
9.4.4 Scheduled Deployments ... 121
9.4.5 Deployment History ... 122

10 Reporting ... 123

10.1 GFI EndPointSecurity GFI ReportPack ... 123
10.2 Generating Digest reports ... 123

11 Managing the Database Backend ... 126

11.1 Maintaining the database backend ... 126
11.2 Using an existing SQL Server instance ... 128

12 Alerting Options ... 129

12.1 Configuring alerting options ... 129
12.2 Configuring the alerts administrator account ... 131
12.3 Configuring alerts recipients ... 135
12.3.1 Creating alert recipients ... 135
12.3.2 Editing alert recipient properties ... 135
12.3.3 Deleting alert recipients ... 135
12.4 Configuring groups of alert recipients ... 135
12.4.1 Creating groups of alert recipients ... 136
12.4.2 Editing group of alert recipients properties ... 136
12.4.3 Deleting groups of alert recipients ... 136

13 Configuring GFI EndPointSecurity ... 138

13.1 Configuring advanced options ... 138
13.2 Configuring user messages ... 140
13.3 Configuring GFI EndPointSecurity updates ... 141

14 Miscellaneous ... 143

14.1 Product licensing ... 143
14.2 Uninstalling GFI EndPointSecurity ... 143
14.2.1 Uninstalling GFI EndPointSecurityagents ... 143
14.2.2 Uninstalling GFI EndPointSecurityapplication ... 145
14.3 Product version information ... 146

15 Troubleshooting and Support ... 147

16 Glossary ... 150

17 Index ... 154

List of Figures

Screenshot 1: Navigating GFI EndPointSecurity user interface 20
Screenshot 2: GFI EndPointSecurity installation: domain administrator account setup 24
Screenshot 3: GFI EndPointSecurity installation: license key details 24
Screenshot 4: Navigating GFI EndPointSecurity user interface 28
Screenshot 5: Selecting control entities 31
Screenshot 6: Selecting device categories to assign permissions 31
Screenshot 7: Adding users or groups 32
Screenshot 8: Selecting permission types per user or group 32
Screenshot 9: Adding computers manually 38
Screenshot 10: Auto Discovery options - Auto Discovery tab 40
Screenshot 11: Auto Discovery options - Discovery Area tab 41
Screenshot 12: Auto Discovery options - Actions tab 42
Screenshot 13: Logon Credentials dialog options 43
Screenshot 14: Creating a new policy - General settings 45
Screenshot 15: Creating a new policy - Controlled Categories and Ports settings 46
Screenshot 16: Controlled Device Categories options 47
Screenshot 17: Controlled connectivity ports options 48
Screenshot 18: Creating a new policy - Global Permissions settings 49
Screenshot 19: Assign Protection Policy Options 52
Screenshot 20: Deploying a policy immediately - Deployment sub-tab 53
Screenshot 21: Schedule deployment options 54
Screenshot 22: Deployment History area 55
Screenshot 23: Agent's Status area 55
Screenshot 24: Controlled Device Categories options 58
Screenshot 25: Controlled connectivity ports options 59
Screenshot 26: Power users options 60
Screenshot 27: Add permissions options - Control entities 61
Screenshot 28: Add permissions options - Device categories 62
Screenshot 29: Add permissions options - Users 62
Screenshot 30: Add permissions options - Users 63
Screenshot 31: Add permissions options - Control entities 64
Screenshot 32: Add permissions options - Connectivity ports 64
Screenshot 33: Add permissions options - Users 65
Screenshot 34: Add permissions options - Control entities 66
Screenshot 35: Add permissions options - Specific devices 67
Screenshot 36: Add permissions options - Users 67
Screenshot 37: Add permissions options - Users 68
Screenshot 38: Protection Policies sub-tab - devices view 69

Screenshot 39: Protection Policies sub-tab - users view 69
Screenshot 40: Protection Policies sub-tab - Security area 70
Screenshot 41: Black list options 71
Screenshot 42: Select Devices options 72
Screenshot 43: Select Devices options - Select device serials 73
Screenshot 44: Select Devices options - Edit Device serials 74
Screenshot 45: White list options 75
Screenshot 46: Select Devices options 75
Screenshot 47: Select Devices options - Select device serials 76
Screenshot 48: Select Devices options - Edit Device serials 77
Screenshot 49: Devices Temporary Access icon 78
Screenshot 50: GFI EndPointSecurityTemporary Access tool 78
Screenshot 51: Grant temporary access options - Request code 79
Screenshot 52: Grant temporary access options - Device categories and connection ports 80
Screenshot 53: Grant temporary access options - Time restrictions 80
Screenshot 54: File-type Filter options 82
Screenshot 55: File-type Filter and user options 83
Screenshot 56: Content awareness options 84
Screenshot 57: Add a new template 85
Screenshot 58: Selecting users or groups 85
Screenshot 59: Managing templates 86
Screenshot 60: File options 87
Screenshot 61: File-type Filter and user options 88
Screenshot 62: Encryption options - General tab 89
Screenshot 63: Encryption options - Permissions tab 89
Screenshot 64: Encryption options - File-type Filter tab 90
Screenshot 65: Encryption options - General tab 91
Screenshot 66: Encryption options -Security tab 92
Screenshot 67: Encryption options - Users tab 93
Screenshot 68: Encryption options - Traveler tab 94
Screenshot 69: Logging Options - General tab 95
Screenshot 70: Logging Options - Filter tab 96
Screenshot 71: Alerting Options - General tab 97
Screenshot 72: Alerting Options - Configuring users and groups 98
Screenshot 73: Alerting Options - Filter tab 99
Screenshot 74: Running a device scan - Logon credentials tab 101
Screenshot 75: Running a device scan - Scan device categories tab 102
Screenshot 76: Running a device scan - Scan ports tab 103
Screenshot 77: Computers area 104
Screenshot 78: Devices list area 104

Screenshot 79: Devices list area - Add device to devices database 105
Screenshot 80: Statistics sub-tab 106
Screenshot 81: Protection Status area 107
Screenshot 82: Device Usage by Device Type area 107
Screenshot 83: Device Usage by Connectivity Port area 108
Screenshot 84: Activity Log sub-tab 109
Screenshot 85: Activity Log sub-tab - Advanced filtering 110
Screenshot 86: Logs Browser sub-tab 111
Screenshot 87: Query Builder options 112
Screenshot 88: Risk Assessment sub-tab 114
Screenshot 89: Statistics sub-tab 116
Screenshot 90: Protection Status area 116
Screenshot 91: Device Usage by Device Type area 117
Screenshot 92: Device Usage by Connectivity Port area 117
Screenshot 93: Status sub-tab 118
Screenshot 94: Deployment sub-tab 120
Screenshot 95: Current Deployments area 121
Screenshot 96: Queued Deployments area 121
Screenshot 97: Scheduled Deployments area 121
Screenshot 98: Deployment History area 122
Screenshot 99: Digest Report options - General tab 124
Screenshot 100: Digest Report options - Details tab 125
Screenshot 101: Maintenance options 127
Screenshot 102: Change Database Backend 128
Screenshot 103: Alerting Options - Email tab 129
Screenshot 104: Alerting Options - Network tab 130
Screenshot 105: Alerting Options - SMS tab 131
Screenshot 106: EndPointSecurityAdministrator Properties options - General tab 132
Screenshot 107: EndPointSecurityAdministrator Properties options - Working Hours tab 133
Screenshot 108: EndPointSecurityAdministrator Properties options - Alerts tab 134
Screenshot 109: EndPointSecurityAdministrator Properties options - Member Of tab 134
Screenshot 110: Creating New Group options 136
Screenshot 111: Advanced Options - Communication tab 138
Screenshot 112: Advanced Options - Deployment tab 139
Screenshot 113: Advanced Options - Agent Security tab 140
Screenshot 114: Custom Messages dialog options 141
Screenshot 115: General tab - Updates 142
Screenshot 116: Editing license key 143
Screenshot 117: Computers sub-tab - delete computer(s) 144
Screenshot 118: Deployment sub-tab 145

Screenshot 119: Uninstallation information message 146
Screenshot 120: Specifying contact and purchase details 148
Screenshot 121: Specifying issue details and other relevant information to recreate the problem 148
Screenshot 122: Gathering machine information 148
Screenshot 123: Finalizing the Troubleshooter wizard 148

List of Tables

Table 1: Terms and conventions used in this manual 11
Table 2: GFI EndPointSecurityfeatures 13
Table 3: Deployment and Monitoring protection policy 15
Table 4: Deployment and Monitoring protection policy 17
Table 5: Deployment and Monitoring protection policy 17
Table 6: System requirements - Hardware 21
Table 7: Auto Discovery settings 26
Table 8: Auto Discovery settings 26
Table 9: Database backend options 27
Table 10: Add Computer(s) dialog options 38
Table 11: Logon credentials options 43
Table 12: Auto Discovery settings 50
Table 13: File options - User options 87
Table 14: Volume encryption - Security options 92
Table 15: Volume encryption - User options 93
Table 16: Volume encryption - Traveler options 94
Table 17: Database maintenance options 127
Table 18: Update options 142
Table 19: Troubleshooting - Common issues 147

1 Introduction

The proliferation of consumer devices such as iPods, USB devices and smartphones has increased the risk of deliberate and/or unintentional data leaks and other malicious activity. It is very simple for an employee to copy large amounts of sensitive data onto an iPod or USB stick, or to introduce malicious and illegal software onto your network through these devices. GFI EndPointSecurityquickly and easily helps you combat these critical threats without needing to lock down all ports and disturbing your daily operations.

Topics in this chapter

1.1 Portable media device threats 11

1.2 About GFI EndPointSecurity 12

1.3 Components of GFI EndPointSecurity 12

1.4 Key Features 13

1.5 How GFI EndPointSecurity works - Deployment and Monitoring 14

1.6 How GFI EndPointSecurity works - Device Access 16

1.7 How GFI EndPointSecurityworks - Temporary Access 17

1.8 Supported device categories 18

1.9 Supported connectivity ports 19

1.10 Navigating the Management Console 19

1.0.1 Terms and conventions used in this guide

Table 1: Terms and conventions used in this manual

Term	Description
	Additional information and references essential for the operation of GFI EndPointSecurity.
	Important notifications and cautions regarding potential issues that are commonly encountered.
>	Step by step navigational instructions to access a specific function.
Bold text	Items to select such as nodes, menu options or command buttons.
Italics text	Parameters and values that you must replace with the applicable value, such as custom paths and filenames.
`Code`	Indicates text values to key in, such as commands and addresses.

1.1 Portable media device threats

The key advantage of removable media devices (or portable devices) is easy access. In theory, this may be of great advantage for organizations, but still, it is a well-reported fact that access and security are at opposite ends of the security continuum.

Developments in removable media technology are escalating. Different versions of portable devices, such as flash memory, have increased in:

- Better storage capacity
- Improved performance
- Easier and faster to install
- Physically small enough to carry in a pocket.

As a result, internal users may deliberately or accidentally:

- Take away sensitive data
- Expose confidential information
- Introduce malicious code (example: viruses, Trojans) that can bring the entire corporate network down
- Transfer inappropriate or offensive material on to corporate hardware
- Make personal copies of company data and intellectual property
- Get distracted during work hours.

In an attempt to control these threats, organizations have started to prohibit the use of (personally-owned) portable devices at work. Best practice dictates that you must never rely on voluntary compliance and the best way to ensure complete control over portable devices is by putting technological barriers.

1.2 About GFI EndPointSecurity

GFI EndPointSecurity is the solution that helps you maintain data integrity by preventing unauthorized access and transfer of content to and from the following devices or connection ports:

- USB Ports (example: Flash and Memory card readers, pen drives)
- Firewire ports (example: digital cameras, Firewire card readers)
- Wireless data connections (example: Bluetooth and Infrared dongles)
- Floppy disk drives (internal and external)
- Optical drives (example: CD, DVD)
- Magneto Optical drives (internal and external)
- Removable USB hard-disk drives
- Other drives such as Zip drives and tape drives (internal and external).

Through its technology, GFI EndPointSecurity enables you to allow or deny access and to assign 'full' or 'read only' privileges to:

- Devices (example: CD/DVD drives, PDAs)
- Local or Active Directory users/user groups.

With GFI EndPointSecurity you can also record the activity of all devices or connection ports being used on your target computers (including the date/time of usage and by whom the devices were used).

1.3 Components of GFI EndPointSecurity

When you install GFI EndPointSecurity, the following components are set up:

- GFI EndPointSecurity Management Console Management Console
- GFI EndPointSecurity Agent.

1.3.1 GFI EndPointSecurity Management Console

Through the Management Console, you can:

- Create and manage protection policies and specify which device categories and connectivity ports are to be controlled
- Remotely deploy protection policies and agents on to your target computers Grant temporary access to target computers to use specific devices
- View the device protection status of every computer that is being monitored
- Carry out scans on target computers to identify devices currently or previously connected
- Check logs and analyze what devices have been connected to every network computer
- Keeps track of which computers have an agent deployed and which agents need to be updated.

1.3.2 GFI EndPointSecurity Agent

The GFI EndPointSecurityagent is a client-side service responsible for the implementation of the protection policies on target computer(s). This service is automatically installed on the remote network target computer after the first deployment of the relevant protection policy through the GFI EndPointSecurity management console. Upon the next deployments of the same protection policy, the agent will be updated and not re-installed.

1.4 Key Features

GFI EndPointSecurity offers the following main features:

Table 2: GFI EndPointSecurityfeatures

GFI EndPointSecurity features	
Group-based protection control	In GFI EndPointSecurity you can configure and place computers into groups that are governed by one protection policy. This allows you to configure a single protection policy and apply it to all the computers that are members of that group.
Granular access control	GFI EndPointSecurity enables you to allow or deny access to a specific device as well as to assign (where applicable) 'full' or 'read only' privileges over every supported device (e.g. CD/DVD drives, PDAs) on a user by user basis.
Scheduled deployment	GFI EndPointSecurity allows you to schedule the deployment of protection policies and any related configuration changes without the need to keep to the GFI EndPointSecurity management console open. The deployment feature also handles failed deployments through automatic rescheduling.
Access control	Apart blocking a range of device categories, GFI EndPointSecurity also allows blocking: » **By file type** - for example, allow the user to read *.doc files but block access to all *.exe files » **By physical port** - all devices connected to particular physical ports, for example, all devices connected to USB ports » **By device ID** - block access to a single device based on the unique Hardware ID of the device. **NOTE** In Microsoft Windows 7, a feature called BitLocker To Go can be used to protect and encrypt data on removable devices. GFI EndPointSecurity performs checks on real file types encrypted with Windows 7 BitLocker To Go.
Device whitelist and blacklist	The administrator can define a list of specific devices that are permanently allowed and others that are permanently banned.

GFI EndPointSecurity features	
Power users	The administrator can specify users or groups who would always have full access to devices that are otherwise blocked by GFI EndPointSecurity.
Temporary access	The administrator is able to grant temporary access to a device (or group of devices) on a particular computer. This feature allows the administrator to generate an unlock code that the end-user can use to obtain a time-limited access to a particular device or port, even when the GFI EndPointSecurity agent is not connected to the network.
Status dashboard	The dashboard's user interface shows the statuses of live and deployed agents, database and alerting servers, the GFI EndPointSecurity service as well as statistical data with charts. The main application keeps track of the live agent status by communicating with its deployed agents. Maintenance tasks are performed automatically once an agent goes online.
Active Directory deployment through MSI	From the GFI EndPointSecurity management console it is possible to generate MSI files that can be later deployed using the Group Policy Object (GPO) feature within the Active Directory or other deployment options. An MSI file will contain all the security settings configured in a particular protection policy.
Agent management password	Agent management functions (such as update and un-install) are protected by a user-configurable password. This means that any other GFI EndPointSecurity instances will not have access to the agent management options.
Device discovery	The GFI EndPointSecurity engine can be used to scan and detect the presence of devices on the network, even on computers that are not assigned any protection policy. The information gathered about detected devices can then be used to build security policies and assign access rights for specific devices.
Logs browser	An in-built tool allows the administrator to browse logs of user activity and device usage that is detected by GFI EndPointSecurity.
Alerting	GFI EndPointSecurity allows you to configure e-mail alerts, network messages and SMS messages that can be sent to specified recipients when devices are connected or disconnected, when device access is allowed or blocked and upon service generated events.
Custom messages	When users are blocked from using devices, they are shown popup messages explaining the reasons why the device was blocked. GFI EndPointSecurity allows the customization of these messages.
Database maintenance	To maintain the size of the database backend, GFI EndPointSecurity can be set to backup or delete events older than a custom number of hours or days.
Device encryption	For maximum security, GFI EndPointSecurity can be configured to encrypt storage devices using AES 256 encryption. Encryption can be enforced on specific computers running agents over the network.
Data leakage risk assessment	The dashboard enables users to see potential data leakage risk for each endpoint. Use the provided tips and perform suggested actions to reduce risks levels.
Content awareness	The content awareness feature enables users to look into files entering the endpoints via removable Devices. Content is identified based on predefined (or custom) regular expressions and dictionary files. By default the feature looks for secure confidential details such as passwords and credit card numbers.

1.5 How GFI EndPointSecurity works - Deployment and Monitoring

GFI EndPointSecurity protection policy deployment and monitoring operations can be divided in the four logical stages described below:

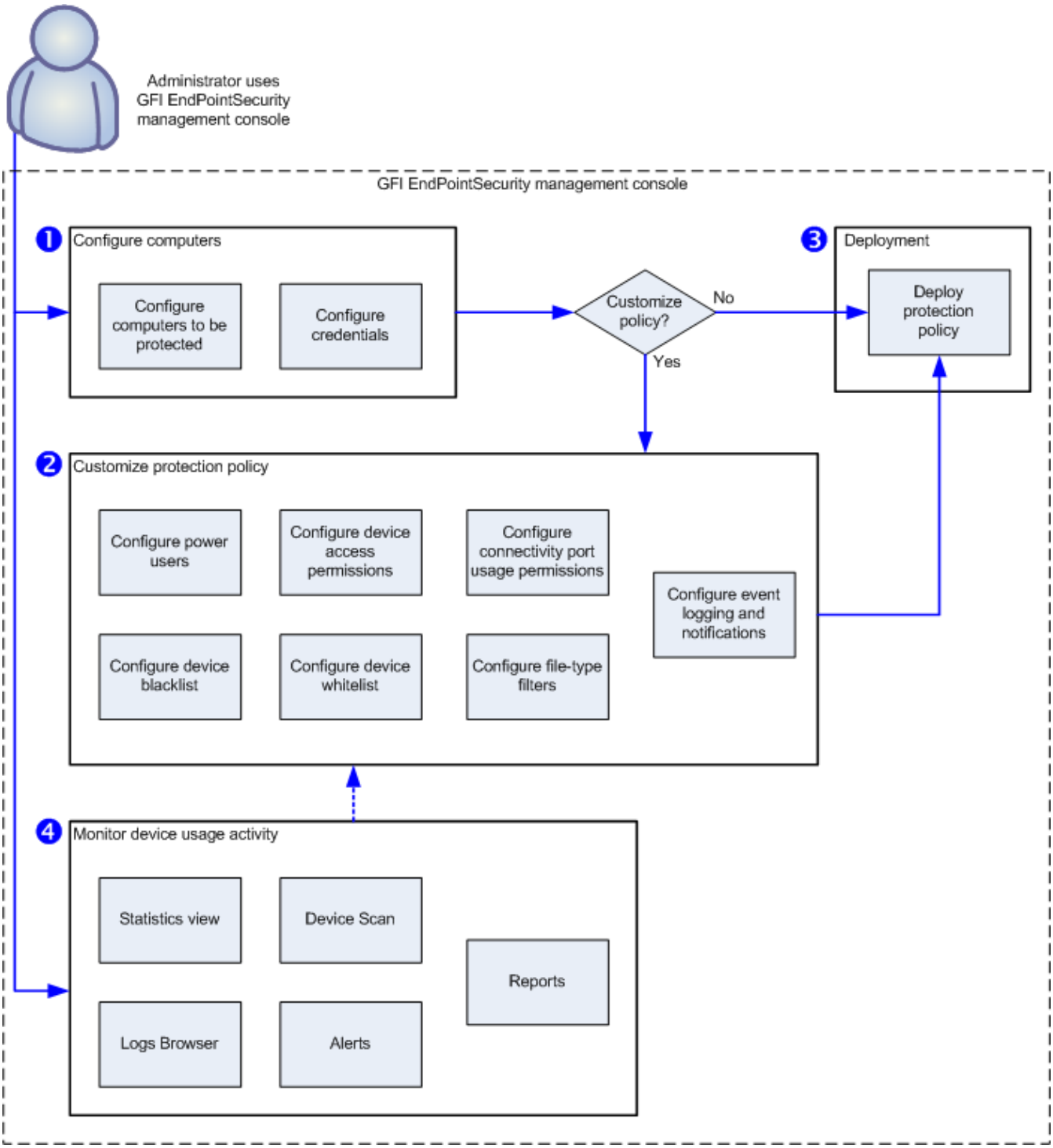


Figure 1: Protection policy - Deployment and Monitoring

The table below describes the stages depicted above:

Table 3: Deployment and Monitoring protection policy

Stage	Description
Stage 1 - Configure computers	The administrator specifies which protection policy is assigned to which computers, and the log-on credentials to be used by GFI EndPointSecurity to access the target computers and deploy the agents.
Stage 2 - Customize protection policy	The administrator can customize a protection policy before or after deploying it. Customization options include the creation of power users, addition of blacklisted/whitelisted devices and device access permissions.

Stage	Description
Stage 3 - Deploy protection policy	The administrator deploys the protection policy. Upon the first deployment of a protection policy, a GFI EndPointSecurity agent is automatically installed on the remote network target computer. Upon the next deployments of the same protection policy, the agent will be updated and not re-installed.
Stage 4 - Monitor device access	When agents have been deployed, the administrator can monitor all device access attempts via the Management Console; receive alerts and generate reports through GFI EndPointSecurity GFI ReportPack.

1.6 How GFI EndPointSecurity works - Device Access

GFI EndPointSecurity device access operations can be divided in three logical stages:

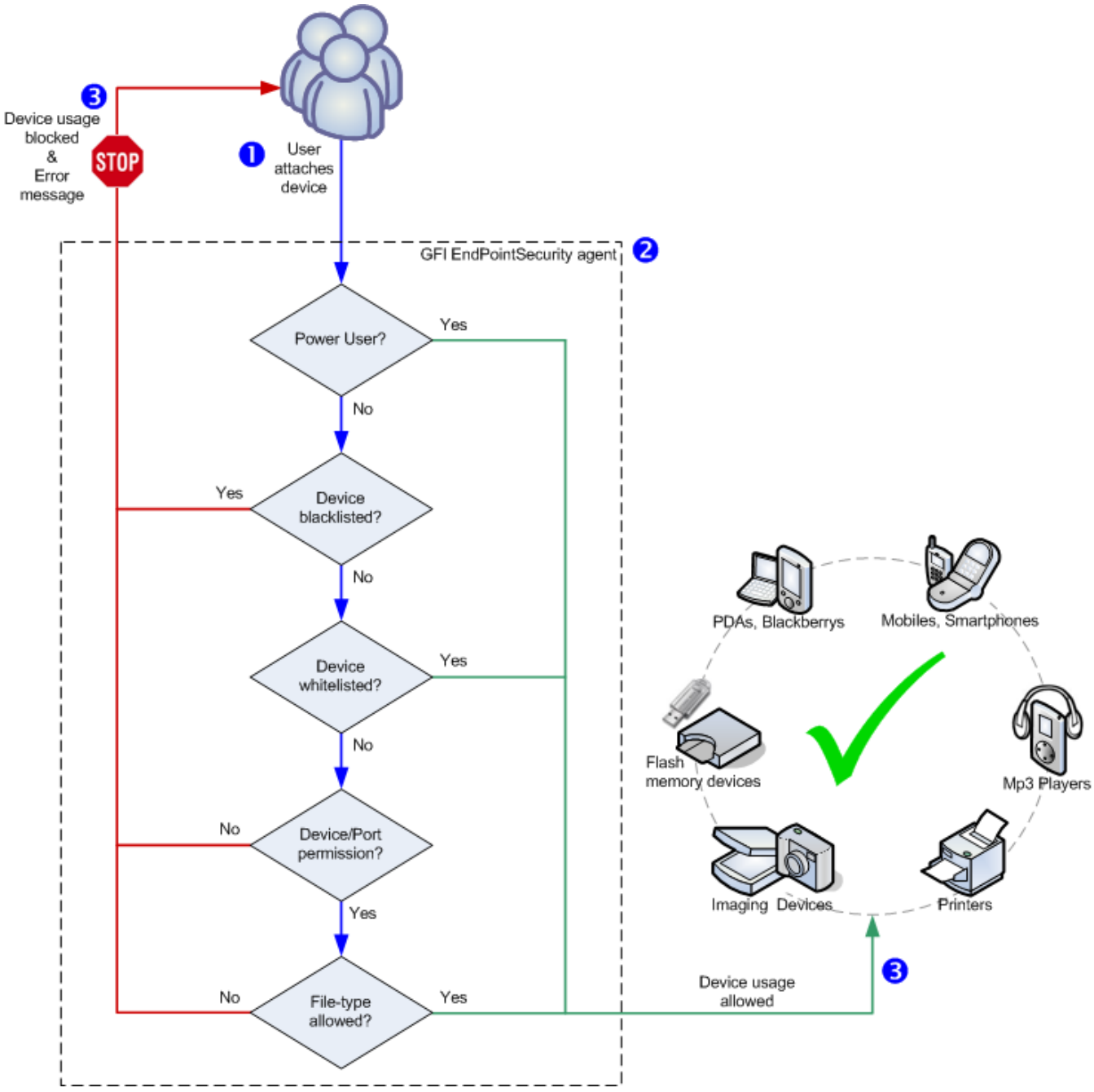


Figure 2: Device access

The table below describes the stages depicted above:

Table 4: Deployment and Monitoring protection policy

Stage	Description
Stage 1 - Device attached to computer	The user attaches a device to a target computer protected by GFI EndPointSecurity.
Stage 2 - Protection policy enforcement	The GFI EndPointSecurity agent installed on the target computer detects the attached device and goes through the protection policy rules applicable to the computer/user. This operation determines whether the device is allowed or blocked from being accessed.
Stage 3 - Device usage allowed/blocked	The user either receives an error message indicating that device usage has been blocked, or else is allowed to access the device.

1.7 How GFI EndPointSecurityworks - Temporary Access

GFI EndPointSecurity temporary access operations can be divided in three logical stages:

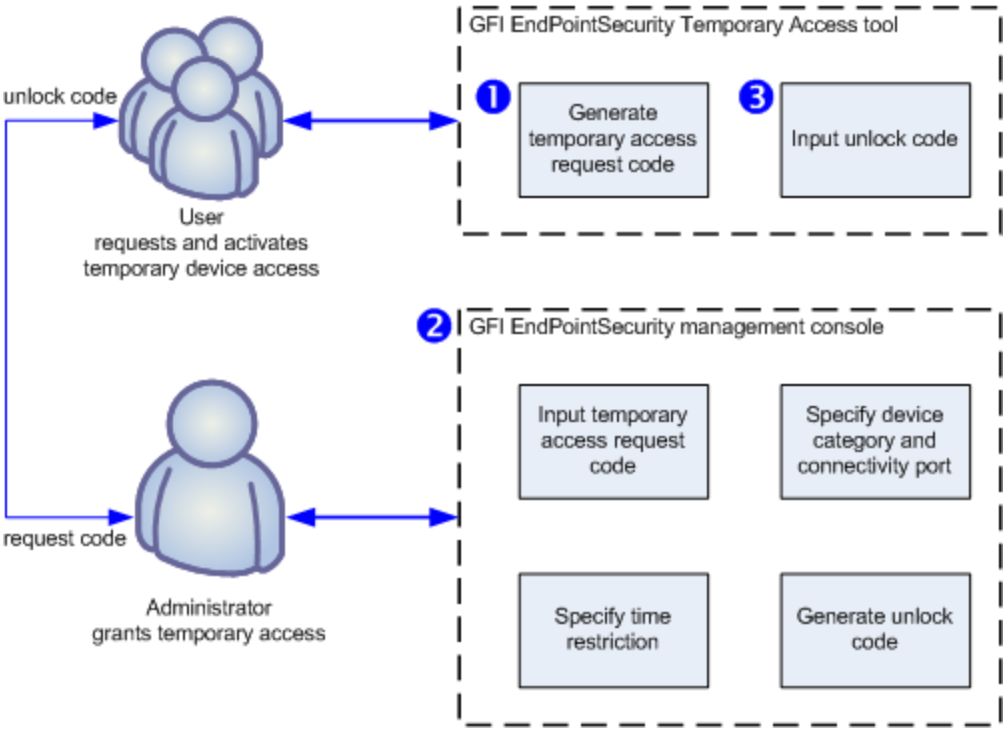


Figure 3: Requesting/granting temporary access

The table below describes the stages depicted above:

Table 5: Deployment and Monitoring protection policy

Stage	Description
Stage 1 - User requests temporary device access	The user executes the GFI EndPointSecurity Temporary Access tool from the computer on which the device is to be accessed. The tool is used to generate a request code, which the user communicates with the administrator. The user also needs to inform the administrator on the device types or connection ports that need to be accessed, and for how long will devices/ports access be required.
Stage 2 - Administrator grants temporary access	The administrator uses the Temporary Access feature within the GFI EndPointSecurity management console to enter the request code, specify devices/ports and time restrictions. An unlock code is generated which the administrator then communicates with the user.
Stage 3 - User activates temporary device access	Once the user receives the unlock code sent by the administrator, this code is entered in the GFI EndPointSecurity Temporary Access tool to activate the temporary access and to be able to use the required devices/ports.

1.8 Supported device categories

In GFI EndPointSecurity devices are organized into the following categories:

Floppy disks

CDs/DVDs

Printers

PDAs, including:

- Pocket PCs
- Smart-phones

Network Adapters, including:

- Ethernet adapters
- Wi-Fi adapters
- Removable adapters (USB, Firewire, PCMCIA)

 Modems, including:

- Smart-phones
- Mobile phones

Imaging Devices:

- Digital cameras
- Webcams
- Scanners

Human Interface Devices:

- Keyboards
- Mice
- Game controllers

 Storage Devices, including:

- USB Pen drives
- Digital Media Players (e.g. MP3/MP4 players)
- Flash and Memory Card Readers
- Multi-drive USB devices (i.e. devices that do not mount as a single drive)

Other Devices:

- Bluetooth dongles/ports
- Infrared dongles/ports

- Zip drives
- Tape drives
- MO (magneto optical) drives (internal and external).

1.9 Supported connectivity ports

GFI EndPointSecurity scans for devices that are or have been connected on the following ports:

USB

Secure Digital (SD)

Firewire

Bluetooth

Infrared

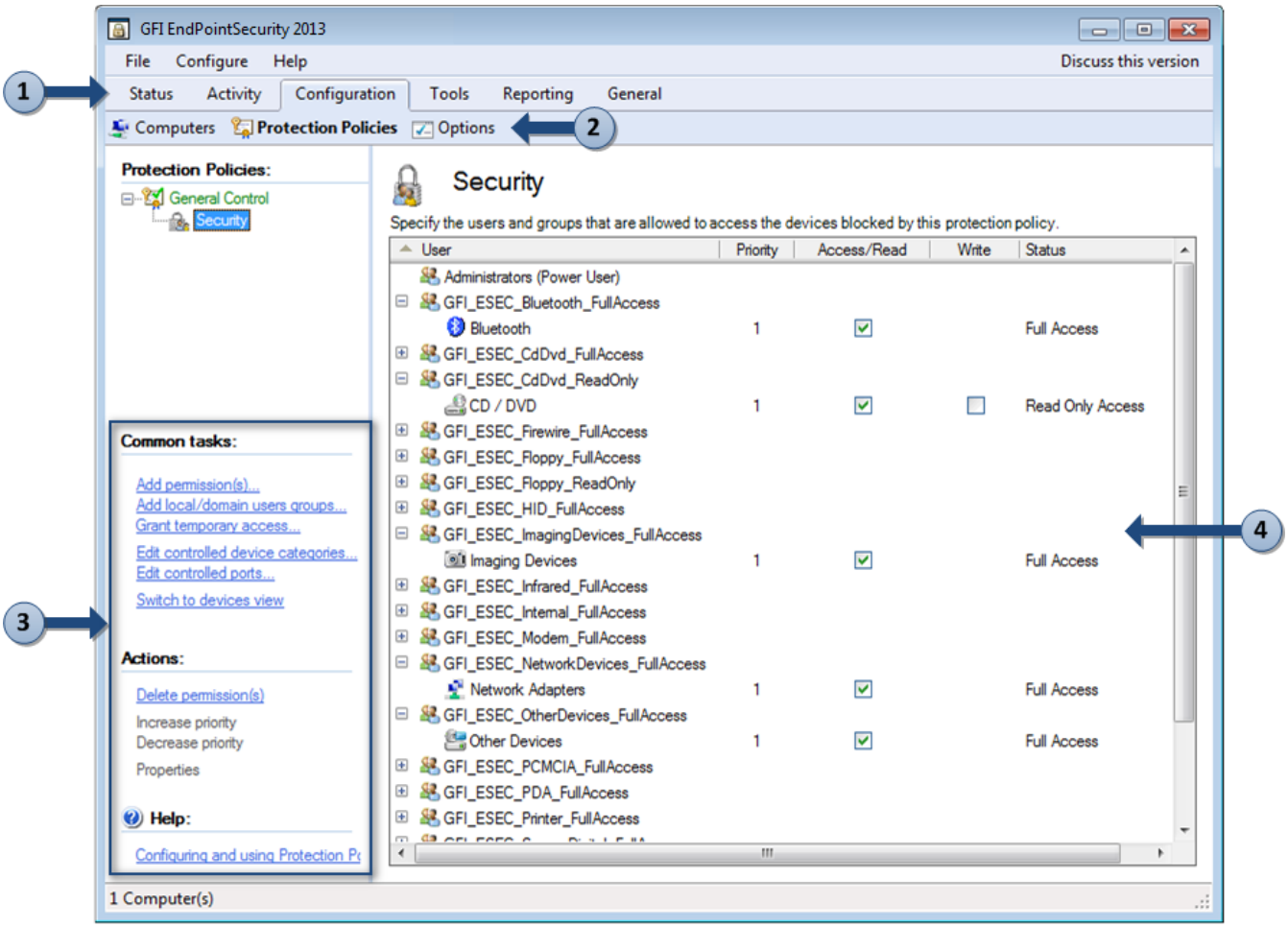
PCMCIA

Serial & Parallel

Internal (example: optical drives connected internally on PCI).

1.10 Navigating the Management Console

GFI EndPointSecurity management console provides you with all the administrative functionality to monitor and manage device access usage.



Screenshot 1: Navigating GFI EndPointSecurity user interface

GFI EndPointSecurity Management Console consists of the sections described below:

Section	Description
1	**Tabs** Navigate between the different tabs of GFI EndPointSecurity management console. The available tabs are: » **Status** - Monitor the status of GFI EndPointSecurity and statistical information on device access. » **Activity** - Monitor devices used on the network. » **Configuration** - Access and configure the default protection policies. » **Scanning** -Scan target computers and discover connected devices » **Reporting** - Download or launch GFI EndPointSecurity GFI ReportPack to generate your reports. » **General** - Check for GFI EndPointSecurity updates, as well as version and licensing detail.
2	**Sub-tabs** Access more settings and/or information about the selected tab from section 1.
3	**Left Pane** Access configuration options provided in GFI EndPointSecurity. The configuration options are grouped into three sections, including **Common Tasks**, **Actions** and **Help**. Available only for some tabs.
4	**Right Pane** Configure the configuration options selected from the left pane. Available only for some tabs.

2 Installing GFI EndPointSecurity

This chapter provides you with information about preparing your network environment to successfully deploy GFI EndPointSecurity.

Topics in this chapter

2.1 System requirements 21

2.2 Upgrading GFI EndPointSecurity 22

2.3 Installing a new instance of GFI EndPointSecurity 23

2.4 Post-install configurations 25

2.5 Navigating the Management Console 27

2.6 Testing your installation 29

2.1 System requirements

Hardware requirements

The table below lists the hardware requirements for GFI EndPointSecurity and GFI EndPointSecurity Agent:

Table 6: System requirements - Hardware

	GFI EndPointSecurity	GFI EndPointSecurity Agent
Processor	Minimum: 2 GHz Recommended: 2GHz	Minimum: 1 GHz Recommended: 1 GHz
RAM	Minimum: 512 MB Recommended: 1 GB	Minimum: 256 MB Recommended: 512 MB
Free space	Minimum: 100 MB Recommended: 100 MB	Minimum: 50 MB Recommended: 50 MB

Supported operating systems (x64/x86)

GFI EndPointSecurity and GFI EndPointSecurity Agent can be installed on a machine running any of the following operating systems:

- Microsoft Windows Server 2012
- Microsoft Windows Small Business Server 2011 (Standard edition)
- Microsoft Windows Server 2008 R2 (Standard or Enterprise edition)
- Microsoft Windows Server 2008 (Standard or Enterprise edition)
- Microsoft Windows Small Business Server 2008 (Standard edition)
- Microsoft Windows Server 2003 (Standard, Enterprise or Web edition)
- Microsoft Windows Small Business Server 2003
- Microsoft Windows 8 (Professional or Enterprise)
- Microsoft Windows 7 (Professional, Enterprise or Ultimate edition)
- Microsoft Windows Vista (Enterprise, Business or Ultimate edition)
- Microsoft Windows XP Professional Service Pack 3.

Agent - Hardware requirements

- Processor: 1GHz processor clock speed or better
- RAM: 256 MB (minimum); 512 MB (recommended)
- Hard Disk: 50 MB of available space

Agent - Software requirements

- Processor: 1GHz processor clock speed or better
- RAM: 256 MB (minimum); 512 MB (recommended)
- Hard Disk: 50 MB of available space

Other software components

GFI EndPointSecurity requires the following software components for a fully functional deployment:

- Microsoft Internet Explorer 5.5 or higher
- Microsoft .NET Framework 2.0 or higher
- Microsoft SQL Server 2000, 2005 or 2008 as the backend database

Note

A database backend is required for storing device access data and for reporting purposes. GFI EndPointSecurity provides the option to either use an available Microsoft SQL Server or else to automatically download and install Microsoft SQL Server 2005 Express on the same computer where GFI EndPointSecurity management console is installed.

Firewall ports

TCP port 1116 (default) - required by GFI EndPointSecurity Agents to notify GFI EndPointSecurity their statuses and to send device access events. Without this port open, the administrator has to either manually monitor events of each target computer or automatically via GFI EventsManager. For more information, refer to http://www.gfi.com/eventsmanager.

2.2 Upgrading GFI EndPointSecurity

Upgrading from GFI EndPointSecurity 3 or later

If you have GFI LanGuard Portable Storage Control, or an earlier version of GFI EndPointSecurity, it is possible to upgrade to the latest version of GFI EndPointSecurity. Upgrading from GFI EndPointSecurity 3 or later to GFI EndPointSecurity2013 is straightforward. The upgrade process is part of the GFI EndPointSecurity2013 installation process, and includes:

- Uninstalling GFI EndPointSecurity 3 or later
- Importing GFI EndPointSecurity 3 configuration settings.

When installing GFI EndPointSecurity you are asked to confirm whether you want to import configurations from the previous version. Click **Yes** to import configurations. You are then prompted to specify which of the following configurations to import:

- Protection Policies:
  - Computer

- Security settings

» Options:

- Logging options
- Database options.

Upgrading from GFI LanGuard Portable Storage Control

If the computer on which you are installing GFI EndPointSecurity is protected by a GFI LanGuardPortable Storage Control agent, you first need to uninstall that agent. To do this:

1. Open GFI LanGuard Portable Storage Control configuration console.

2. Delete the agent from the computer where GFI EndPointSecurity will be installed.

> **Note**
>
> This process should be done only for the computer where GFI EndPointSecurity will be installed.

3. Close the GFI LanGuard Portable Storage Control configuration console application and proceed to installing GFI EndPointSecurity.

4. When installing GFI EndPointSecurity, you are asked to confirm whether you want to import configurations from the previous version. Click **Yes** to import configurations.

> **Note**
>
> GFI LanGuard Portable Storage Control agents that were protecting your computers will be automatically added to a protection policy called **LegacyAgents** in GFI EndPointSecurity.

2.3 Installing a new instance of GFI EndPointSecurity

To install GFI EndPointSecurity:

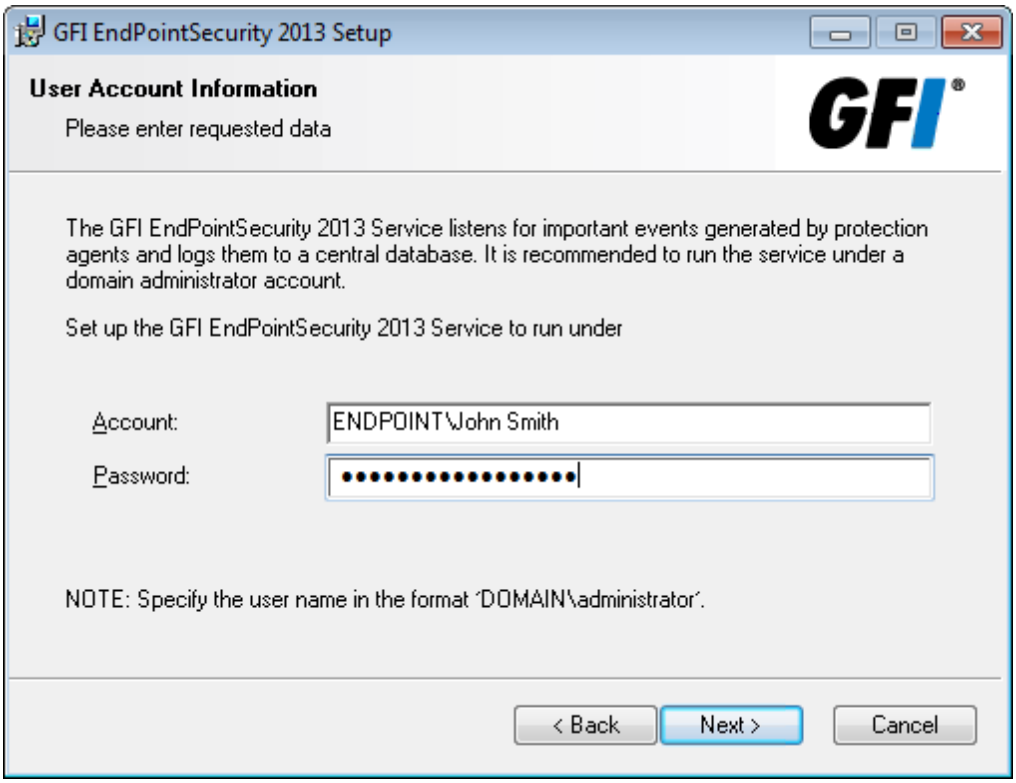
1. Logon the machine where GFI EndPointSecurity is going to be installed, using administrative privileges.

2. Double-click the GFI EndPointSecurity executable file.

2. Select the language you want to install and click **OK**.

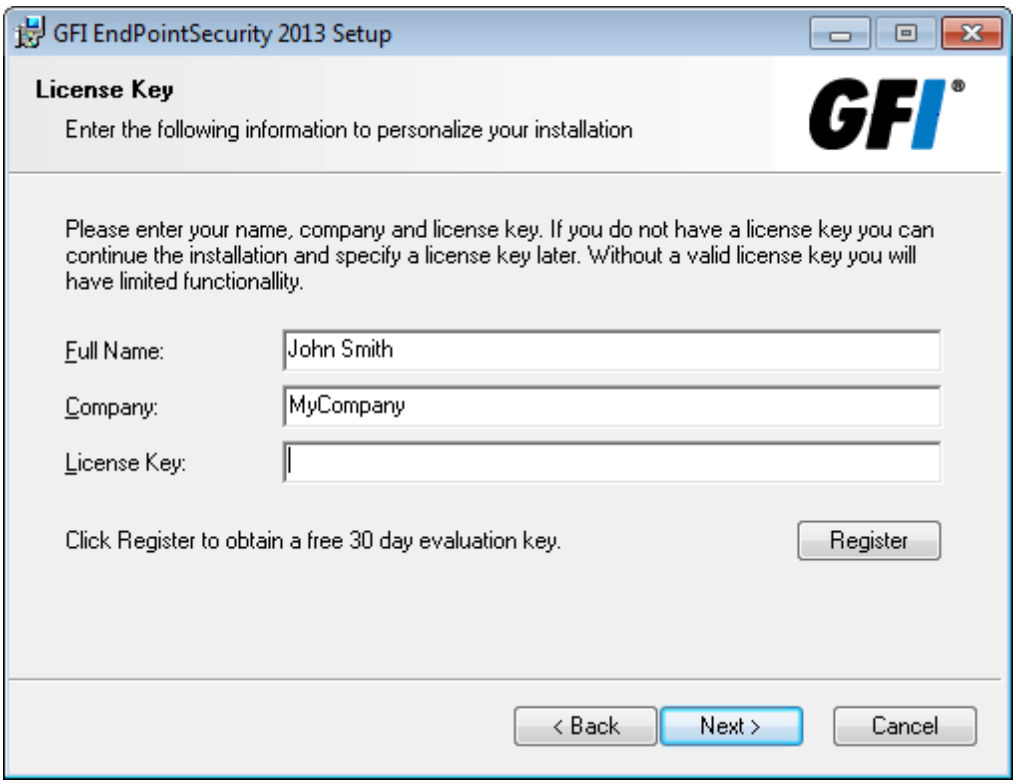
3. Click **Next** at the Welcome screen to start setup.

4. Read carefully the End-User License Agreement. If you agree to the terms laid out in the agreement, select **I accept the license agreement** and click **Next**.



Screenshot 2: GFI EndPointSecurity installation: domain administrator account setup

5. Key in the logon credentials of an account with administrative privileges and click **Next** to continue.



Screenshot 3: GFI EndPointSecurity installation: license key details

6. Key in the **Full Name** and **Company**. If you have a license key, update the **License Key** details and click **Next**.

Note

The license key can be keyed in after installation or expiration of the evaluation period of GFI EndPointSecurity. For more information refer to Product licensing.

7. Key in or browse to select an alternative installation path or click **Next** to use the default path and proceed with the installation.

8. Click **Back** to re-enter installation information or click **Next** and wait for the installation to complete.

9. Upon installation completion, enable or disable the Launch GFI EndPointSecurity checkbox and click **Finish** to finalize installation.

2.4 Post-install configurations

On the initial launch of GFI EndPointSecurity management console, the Quick Start wizard is automatically launched. This enables you to configure important GFI EndPointSecurity settings for first time use.

The Quick Start wizard consists of the following steps and guides you to configure:

- Risk Assessment
- Automatic discovery
- Power users
- Users groups
- Database backend.

Note

The Quick Start Wizard can be re-launched from **File > Quick Start Wizard**.

To use the Quick Start Wizard:

1. Click **Next** at the wizard welcome screen.
2. From **Risk Assessment**, select/unselect **Start a Risk Scan** to enable / disable the function to start a scan on your network to determine the risk level.
3. (Optional) Click **Risk scan settings...** and configure settings from the tabs described below:

Table 7: Auto Discovery settings

Tab	Description
Scan Area	Select the target area on which GFI EndPointSecurity scans the computers on the network. » **Current domain/workgroup** - GFI EndPointSecurity searches for new computers within the same domain/workgroup where it is installed » **The following domains/workgroups** - Select this option and click **Add**. Specify the domains where GFI EndPointSecurity searches for new computers and click **OK**. » **Entire network except** - Select this option and click **Add**. Specify the domain/workgroup that should be excluded during auto discovery and click **OK**. » **IP range** - Select this option and click **Add**. Specify the range of IP addresses that should be included or excluded during auto discovery and click **OK**. » **Computer list** - Select this option and click **Add**. Specify the domain/workgroup that should be included or excluded during auto discovery and click **OK**.
Logon Credentials	Enable/disable **Logon using credentials below** and specify a set of credentials that GFI EndPointSecuritywill use to access computers that will be scanned.
Scan Device Categories	Select the device categories that GFI EndPointSecuritywill include in the scan.
Scan ports	Select the device connection ports that GFI EndPointSecuritywill include in the scan.

4. Click **Apply** and **OK** to close the Risk Assessment dialog and click **Next** at the Quick Start Wizard.
5. From **Auto Discovery**, select/unselect **Enable Auto Discovery** to turn on/off auto discovery. When Auto Discovery is enabled, GFI EndPointSecurity periodically scans your network for new computers.
6. Select/unselect **Install agents on discovered computers** to turn on/off automatic deployment of GFI EndPointSecurity Agents on newly discovered computers.
7. (Optional) Click **Auto discovery settings...** and configure settings from the tabs described below:

Table 8: Auto Discovery settings

Tab	Description
Auto Discovery	Enable/disable auto discovery and configure a schedule when GFI EndPointSecurity scans your network for new computers.
Discovery Area	Select where GFI EndPointSecurity searches for new computers. Select from: » **Current domain/workgroup** - GFI EndPointSecurity searches for new computers within the same domain/workgroup where it is installed » **The following domains/workgroups** - Select this option and click **Add**. Specify the domains where GFI EndPointSecurity searches for new computers and click **OK**. » **Entire network except** - Select this option and click **Add**. Specify the domain/workgroup that should be excluded during auto discovery and click **OK**.
Actions	Configure the actions taken by GFI EndPointSecurity when a new computer is discovered. Also select the policy that these settings apply to.

8. Click **Apply** and **OK** to close the Auto Discovery dialog and click **Next** at the Quick Start Wizard.
9. From **Power Users** select/unselect **Set GFI EndPointSecurity Power Users** to enable/disable power users features. Members of the power users group have access to any connected device effected by this policy.
10. Click **Select Power Users...** and from the Power Users dialog, click **Add...** to add users from your domain/workgroup.
11. Click **Apply** and **OK** to close the Power Users dialog and click **Next** at the Quick Start Wizard.

12. From **Users Groups**, select/unselect **Configure Users Groups** to create domain/workgroup users and bind them to device categories and connectivity ports settings selected in the next step.
13. Click **Select which Users Groups to create...**. From the Configure Users Groups dialog, select the devices and/or connection ports for which users are created on. To manage every supported device and port from this policy, click **Select All**.
14. Click **Close** to close the **Configure Users Groups** and click **Next** at the Quick Start Wizard.
15. From Database, select the database type you want to use as the database backend. Select from the options described below:

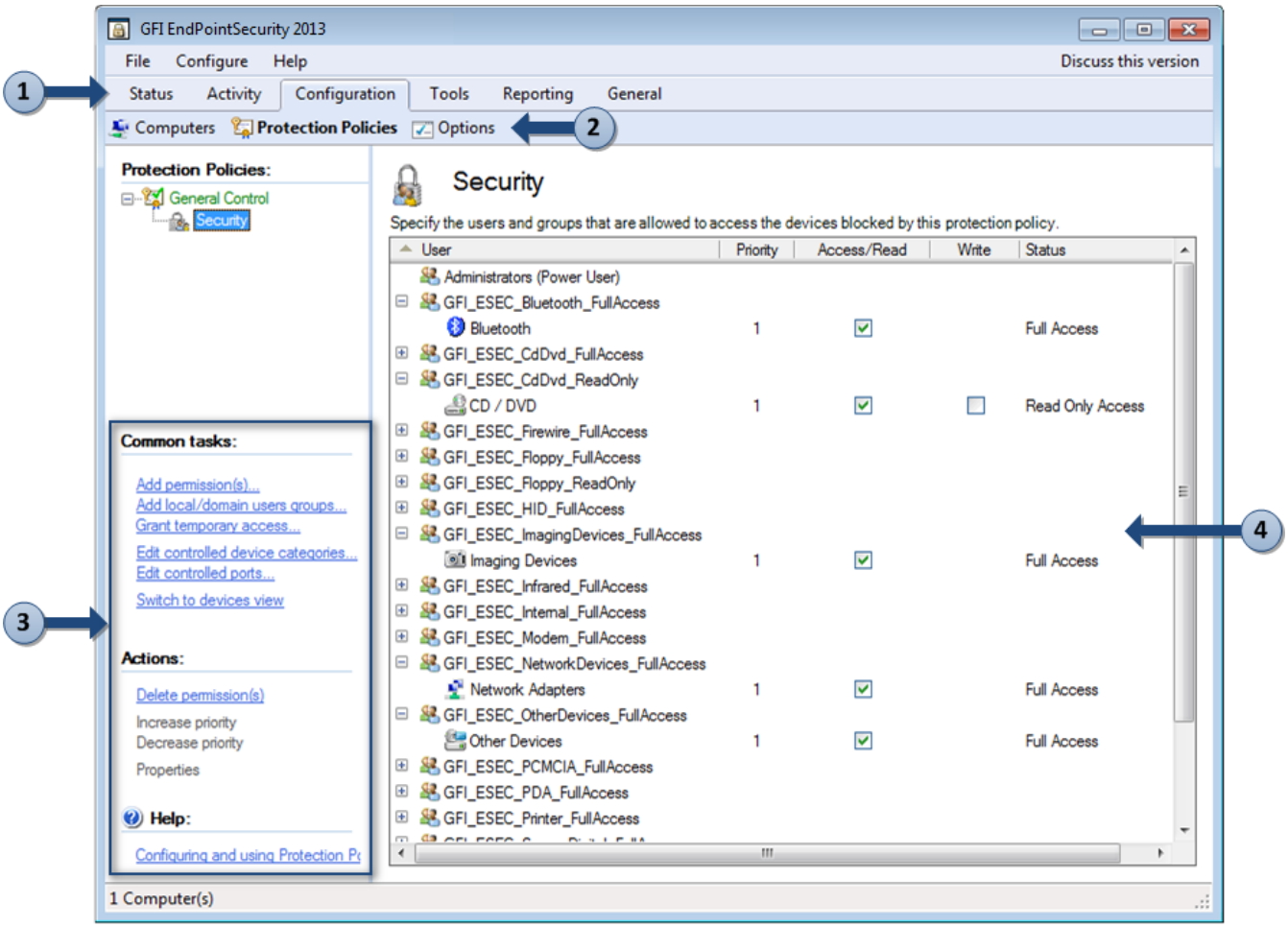
Table 9: Database backend options

Option	Description
Don't configure the database at this time	Finalize the Quick Start Wizard and configure the database backend later. For more information, refer to ACM
Use an already installed SQL Server instance	Use an instance of Microsoft SQL Server already installed on the same machine you are installing GFI EndPointSecurity or any other machine on the network.
Install a local instance of SQL Express Edition	Select this option to download and install an instance of Microsoft SQL Server Express on the same machine you are installing GFI EndPointSecurity. An Internet connection is required.

16. (Optional) Click **Advanced database settings...** to specify the SQL Server address, database name, logon method and the respective credentials. Click **Apply** and **OK** to close the Database Backend dialog.
17. Click **Next** and wait for the settings to be applied. Click **Finish** to close the Quick Start Wizard.

2.5 Navigating the Management Console

GFI EndPointSecurity management console provides you with all the administrative functionality to monitor and manage device access usage.



Screenshot 4: Navigating GFI EndPointSecurity user interface

GFI EndPointSecurity Management Console consists of the sections described below:

Section	Description
1	**Tabs** Navigate between the different tabs of GFI EndPointSecurity management console. The available tabs are: » **Status** - Monitor the status of GFI EndPointSecurity and statistical information on device access. » **Activity** - Monitor devices used on the network. » **Configuration** - Access and configure the default protection policies. » **Scanning** -Scan target computers and discover connected devices » **Reporting** - Download or launch GFI EndPointSecurity GFI ReportPack to generate your reports. » **General** - Check for GFI EndPointSecurity updates, as well as version and licensing detail.
2	**Sub-tabs** Access more settings and/or information about the selected tab from section 1.
3	**Left Pane** Access configuration options provided in GFI EndPointSecurity. The configuration options are grouped into three sections, including **Common Tasks**, **Actions** and **Help**. Available only for some tabs.
4	**Right Pane** Configure the configuration options selected from the left pane. Available only for some tabs.

2.6 Testing your installation

Once GFI EndPointSecurity is installed and the Quick Start wizard is completed, test your installation to ensure that GFI EndPointSecurity is working correctly. Follow the instructions in this section to verify the correctness of both the GFI EndPointSecurity installation as well as the operations of the shipping default protection policy.

This section contains the following information:

- Test preconditions
- Test case
- Reverting to default settings

2.6.1 Test preconditions

The following test pre-conditions and settings are required ONLY for the purpose of this test:

Device setup

For the following test you require:

- CD/DVD drive connected to the local computer
- CD/DVD disc containing accessible contents (preferably a disc the contents of which were accessible prior to the installation of GFI EndPointSecurity).

> **Note**
>
> Other devices and media may be used, such as Floppy Disks or pen drives.

User accounts

For this test ensure the availability of two user accounts on the same computer where GFI EndPointSecurity is installed:

- One with no administrative privileges
- One with administrative privileges.

Configuration settings

The configuration of the Quick Start wizard allows you to fine tune GFI EndPointSecurity to suit your company's needs which may not match the pre-test settings required by this test. As a result, some GFI EndPointSecurity configuration settings need to be set as indicated below for this test to succeed:

- Ensure the local computer is listed in the **Status > Agents** view. If the local computer is not listed, then manually include it within the computers list. For more information, refer to the GFI EndPointSecurity- Administration and Configuration Manual.
- Ensure the shipping default protection policy is deployed on the local computer and is up-to-date. To verify check in the **Status > Agents** view that:
  - the protection policy is set to General Control
  - the deployment is Up-to-date
  - the local computer is Online.

Note

If the deployment of the agent on to the local computer is not up-to-date, then manually deploy the agent on to it. For more information, refer to the GFI - Administration and Configuration Manual.

» Ensure that the user account with no administrative privileges is not set as a power user in the General Control protection policy (shipping default protection policy).

Note

If the user account is set as a power user, then manually remove it from the power users group of the General Control protection policy (shipping default protection policy). For more information, refer to the GFI EndPointSecurityAdministration and Configuration Manual.

2.6.2 Test case

Accessing a CD/DVD disc

Upon compliance with the previously outlined test pre-conditions, non-administrative users are no longer allowed access to any devices or ports connected to the local computer.

To verify that both the device and media are inaccessible to the non-administrative user:

1. Log in to the local computer as the user with no administrative privileges.

2. Insert the CD/DVD disc in the CD/DVD drive.

3. From **Windows Explorer** locate the CD/DVD drive and confirm that you are unable to view and open the contents stored on the CD/DVD disc.

Assign permissions to user with no administrative privileges

To assign CD/DVD device access permissions to the user with no administrative privileges:

1. Log in to the local computer as the user with administrative privileges.

2. Launch GFI EndPointSecurity.

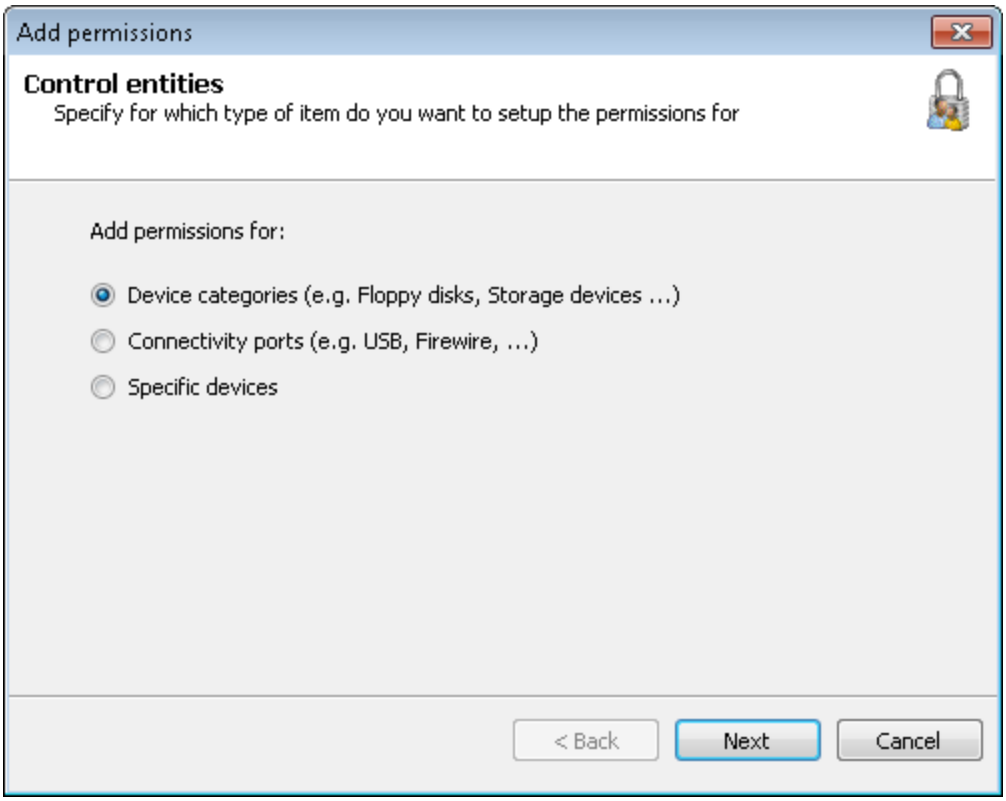
3. Click on the **Configuration** tab.

4. Click on the **Protection Policies** sub-tab.

5. From the left pane, select the **General Control** protection policy.

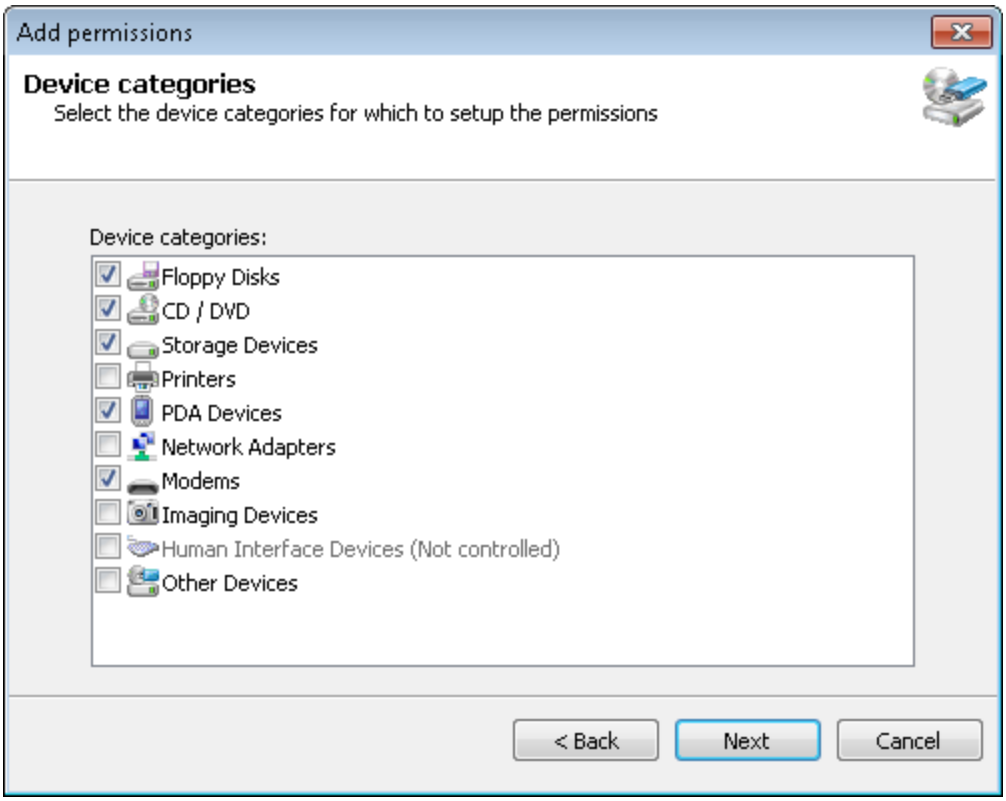
6. Click on the **Security** sub-node.

7. From the left pane, click the **Add permission(s)…** hyperlink in the **Common tasks** section.



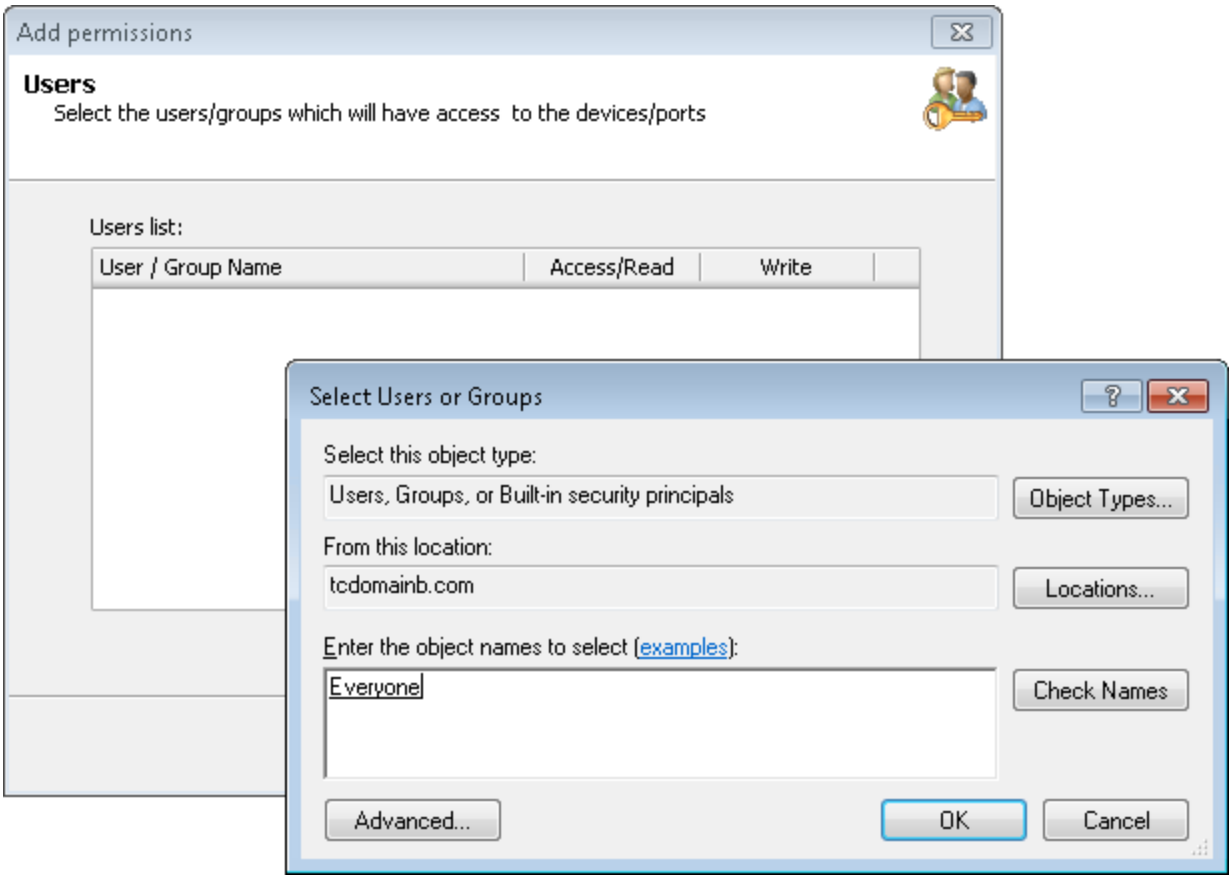
Screenshot 5: Selecting control entities

8. In the **Add permissions...** dialog select the **Device categories** option and click **Next** to continue.



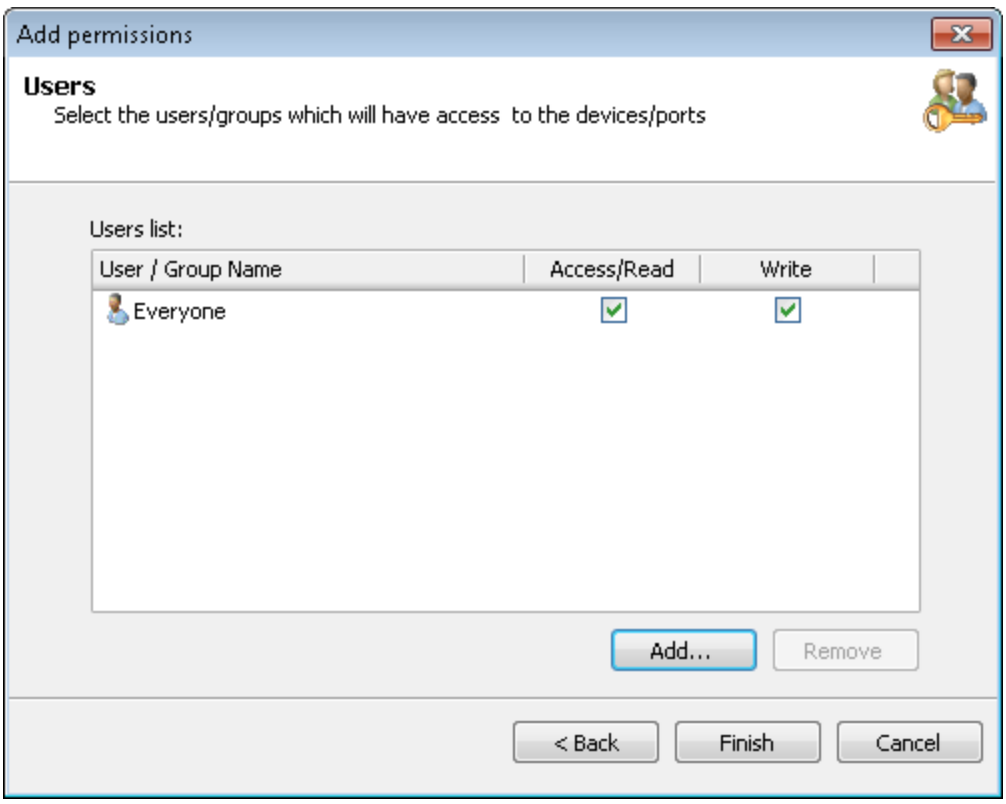
Screenshot 6: Selecting device categories to assign permissions

9. Enable the **CD/DVD** device category, and click **Next**.



Screenshot 7: Adding users or groups

10. Click **Add…** and specify the user with no administrative privileges, to have access to the CD/DVD device category specified in this protection policy, and click **OK**.



Screenshot 8: Selecting permission types per user or group

11. Enable the **Access/Read** and **Write** permissions and click **Finish**.

To deploy the protection policy updates on to the local computer:

1. From the right pane, click on the top warning message to deploy the protection policy updates. The view should automatically change to **Status > Deployment**.

2. From the **Deployment History** area, confirm the successful completion of the update onto the local computer.

Re-accessing a CD/DVD disc

Upon the assignment of user permissions, the specified user with no administrative privileges should now be allowed to access CD/DVD discs through CD/DVD drives connected to the local computer.

To verify that both the device and media are now accessible to the non-administrative user:

1. Log in to the local computer as the user with no administrative privileges.

2. Insert the same CD/DVD disc in the CD/DVD drive.

3. From **Windows Explorer** locate the CD/DVD drive and confirm that you are now able to view and open the contents stored on the CD/DVD disc.

2.6.3 Reverting to default settings

To revert any GFI EndPointSecurity configuration settings back to the pre-test scenario, do the following for the user with no administrative privileges:

1. Remove the user account from the local computer, if it was created only for this test and is no longer required.

2. Manually include the user in the power users list, if it was set as a power user prior to this test. For more information, refer to the GFI EndPointSecurity - Administration and Configuration Manual.

3. Delete the CD/DVD device access permissions to the user, if it was not assigned CD/DVD device access permissions prior to this test. For more information, refer to the GFI EndPointSecurity - Administration and Configuration Manual.

3 Achieving Results

This chapter provides you with step by step instructions about how to block unauthorized devices from the network and secure endpoints using GFI EndPointSecurity. This chapter helps you achieve positive legal compliance results, while ensuring that your network is protected using the most up-to-date vulnerability detection methods and techniques.

Topics in this chapter

3.1 Preventing data leaks and malware infections 34

3.2 Automating network protection 35

3.3 Monitoring network activity from a central location 37

3.1 Preventing data leaks and malware infections

Most data theft happens internally by employees manually transferring data onto removable storage devices. Using unauthorized removable storage devices can expose the network to a higher risk of malware infections. GFI EndPointSecurity enables you to comprehensively control access to portable storage devices with minimal administrative effort. Temporary access can be granted to end-users for a device on a particular computer for a particular timeframe.

1. Deploy agents on computers that require protection

GFI EndPointSecurity Agents are used to secure computers on the network. Agents can be deployed manually, when installing agents on specific computers or automatically when installing agents on every new endpoint discovered on the network. Refer to the following sections for information about:

- Adding computers manually
- Adding computers automatically
- Configuring log on credentials.

2. Create a protection policy to block removable storage

Agents secure computers based on settings of an assigned security policy. You can create as many security policies as required, and each policy can contain different settings for different authorization levels. Refer to the following sections for information about:

- Creating protection policies
- Assigning protection policies
- Deploying policies immediately
- Scheduling policy deployment
- Deploying policies through Active Directory
- Verifying protection policy deployment.

3. Configure protection policy settings

Configure the protection policy to block removable storage devices. This prevents end-users from using devices that allow them to transfer data from and to a computer. Refer to the following sections for information about:

- Configuring controlled device categories
- Configuring access permissions for device categories
- Configuring access permissions for specific devices
- Configuring priorities for permissions
- Viewing access permissions
- Configuring device blacklist.

---

4. Configure notification alerts on attempted breach of the security policy

GFI EndPointSecurity can send notifications to a single or group of recipients when an end-user attempts to breach a security policy. This enables you to immediately take the required actions and terminate unauthorized use of removable storage devices. Refer to the following sections for information about:

- Configuring alerts
- Configuring alerting options
- Configuring the alerts administrator account
- Configuring alerts recipients
- Configuring groups of alert recipients.

---

5. Configure temporary access for genuine use of removable storage devices

If a blocking protection policy is active, GFI EndPointSecurity still enables you to temporary allow access to a device to genuinely transfer data to and from a computer. Refer to the following sections for information about:

- How GFI EndPointSecurity works - Temporary Access
- Configuring power users
- Configuring temporary access privileges
- Configuring device whitelist
- Configuring user messages.

3.2 Automating network protection

After configuring GFI EndPointSecurity, you can automatically protect new computers that are detected on reachable networks. This can be achieved by specifying the domain(s) and/or workgroup (s) that must be scanned for new computers and upon detection of one, GFI EndPointSecurity installs an agent automatically and assigns it the default policy. Policies can be changed from Configuration tab > Computers sub-tab.

---

1. Automatically discover devices on the network

GFI EndPointSecurity enables you to automatically add new computers that are connected to the network. This allows you to scan a specified domain or workgroup and add the computers that are found in it. Refer to the following sections for information about:

- Running a device scan
- Analyzing device scan results
- Adding discovered devices to the database.

---

2. Deploy agents on new discovered devices

GFI EndPointSecurity can be configured to automatically install agents on new computers that are added to the database. An agent must be installed on each computer that requires protection. Refer to the following sections for information about:

- Adding computers automatically
- Configuring advanced options
- Configuring log on credentials.

---

3. (Optional) Configure the protection policy that is assigned to newly discovered devices

If a protection policy is not configured for deployment, create a policy that can be assigned to new agents that are being installed on discovered computers. The default policy must be assigned to a new agent but can be changed from the Configuration tab > Computers sub-tab. Security settings and device behavior are dictated by the policy. Refer to the following section for information about:

- Customizing Protection Policies
- Setting a policy as the default policy.

---

4. Assign protection policies automatically

Configure GFI EndPointSecurity to automatically deploy protection policies on new agents. Refer to the following sections for information about:

- Scheduling policy deployment
- Deploying policies through Active Directory
- Verifying protection policy deployment.

---

5. Monitor device activity

GFI EndPointSecurity enables you to maintain an audit trail of activity logs generated by agents deployed on network computers (event logging must be enabled). The Status and Activity tabs enable you to view statuses and statistical information about endpoints, agents and GFI EndPointSecurity. Refer to the following sections for information about:

- Configuring event logging
- View device usage activity
- View device usage statistics.

3.3 Monitoring network activity from a central location

Agents generate activity logs that are stored in an SQL Server database. GFI EndPointSecurity keeps an audit trail of these logs and provides the information in a set of dashboard views. GFI EndPointSecurity's extensive dashboard views enable you to monitor network activity in real-time, allowing the administrator to take immediate action when a security risk is detected. Configure GFI EndPointSecurity to periodically (daily/weekly/monthly) generate and send reports to IT and management staff for a full analysis view of endpoint security statuses.

1. Analyze network-wide activity

The sub-tabs provided under the Status and Activity tabs enable you to monitor network activity from a central location. These tabs provide you with risk assessment, statistics, statuses, activity logs and deployment information using charts and tables. Refer to the following sections for information about:

- Analyzing risk assessment details
- Analyzing statistics
- Analyzing status information
- Analyzing agent deployment details
- Analyzing activity logs.

2. Generate reports based on activity logs generated by agents on the network

GFI EndPointSecurity contains an extensive list of reports that can be used as they are, or even modified to further suit your reporting requirements. The ReportPack contains both technical reports for IT staff as well as executive reports for management purposes. Refer to the following sections for information about:

- Using GFI EndPointSecurity ReportPack
- Generating digest reports.

3. Maintain the database backend

GFI EndPointSecurity stores event logs in an SQL Server database. In a large network with a lot of activity, the size of the database can grow exponentially and read/write performance between GFI EndPointSecurity and the database may degrade. It is recommended to configure log retention settings to automatically delete old or unwanted events or even create a new database when the current one reaches a specific size. Refer to the following sections for information about:

- Maintaining the database backend
- Using an existing SQL Server instance.

4 Adding Target Computers

GFI EndPointSecurity enables you to specify the computers you intend to deploy agents and protection policies on.

Topics in this chapter

4.1 Adding computers manually 38

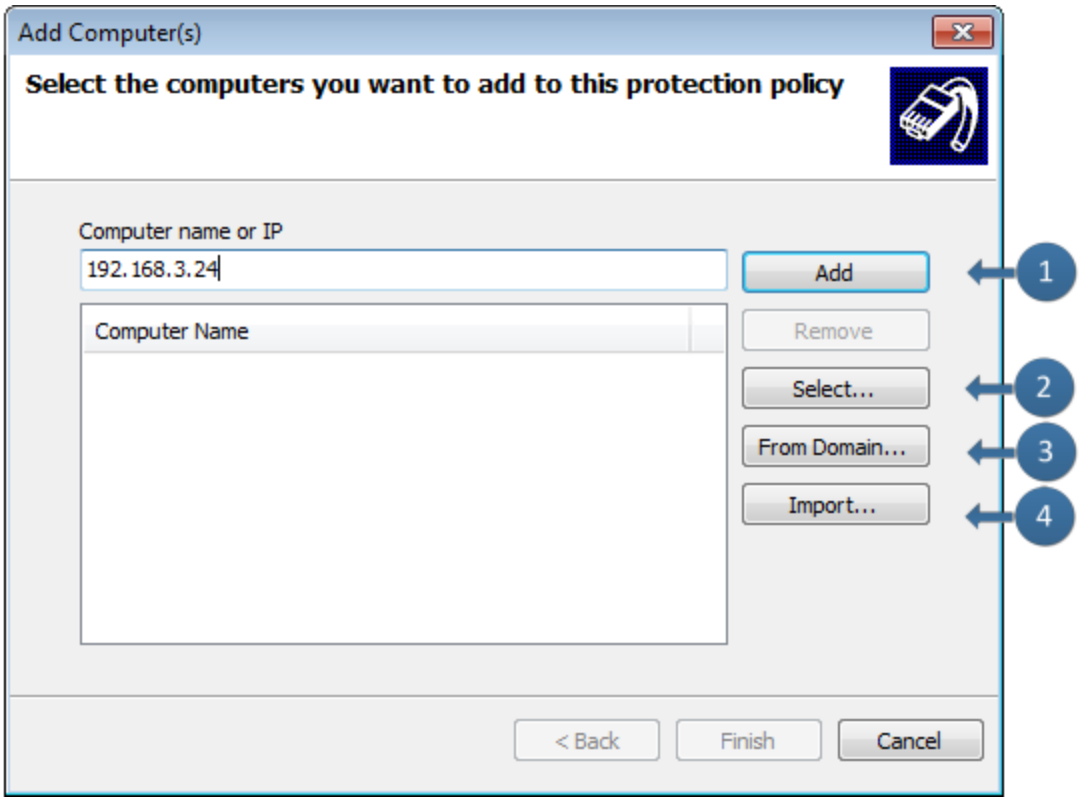
4.2 Adding computers automatically 39

4.3 Configuring log on credentials 42

4.1 Adding computers manually

To manually add a target computer:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Add computer(s)…**.



Screenshot 9: Adding computers manually

3. The table below describes the available options of the **Add Computer(s)** dialog:

Table 10: Add Computer(s) dialog options

Option	Description
1	Key in the name/IP of the target computer to add and click **Add**. Repeat this step for each target computer you want to add to this protection policy.
2	Click **Select…**. In the **Select Computers** dialog select the relevant Domain/Workgroup from the drop-down list and click **Search**. Enable the required computer(s) and click **OK**.

Option	Description
3	Click **From Domain…**. Specify the required computer(s) from within the domain/workgroup where GFI End-PointSecurity resides.
4	Click **Import**. Browse to the location of the text file that contains a list of computers to be imported. **Note** Specify ONLY one computer name/IP per line.

4. Click **Finish**.

4.2 Adding computers automatically

GFI EndPointSecurity enables you to search for and add new computers when they are connected to your network at specified time intervals. This enables you to automatically add computers as soon as they are detected on the network. Through Auto Discovery features, you can configure:

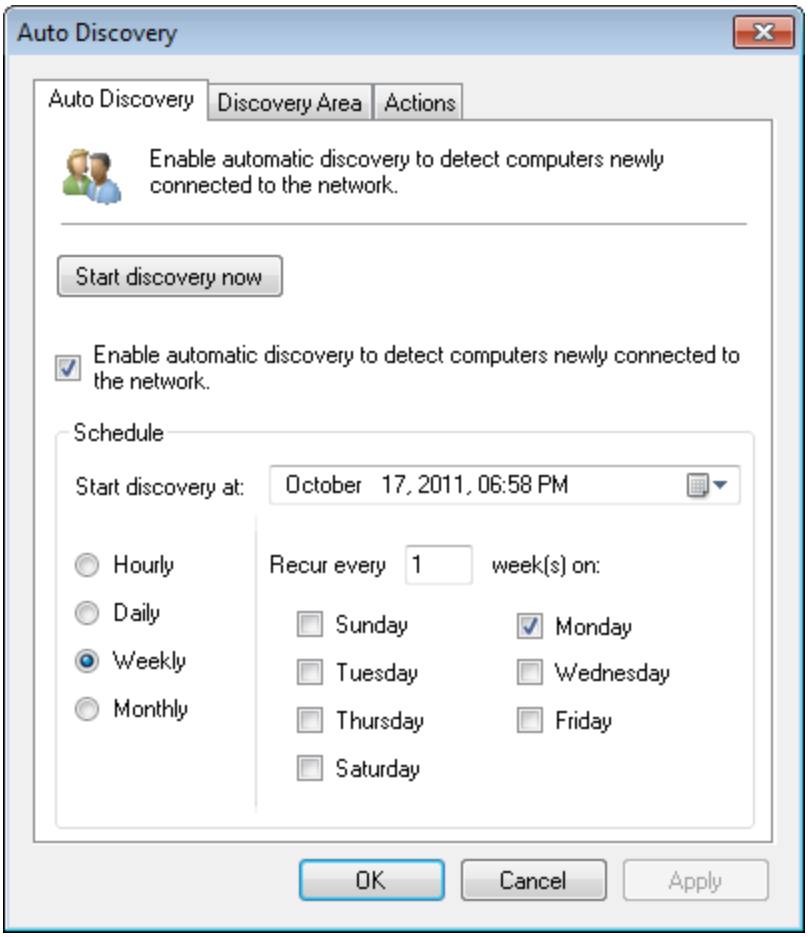
- The frequency and schedule of the searches
- The discovery domain/workgroup to scan
- The policy assigned to newly discovered target computers and the logon credentials.

By default:

- Auto discovery settings are set to scan the Current domain/workgroup (domain/workgroup where GFI EndPointSecurity resides)
- Install agent's settings are set to assign the **General Control** protection policy (shipping default protection policy) on to the newly discovered computers.

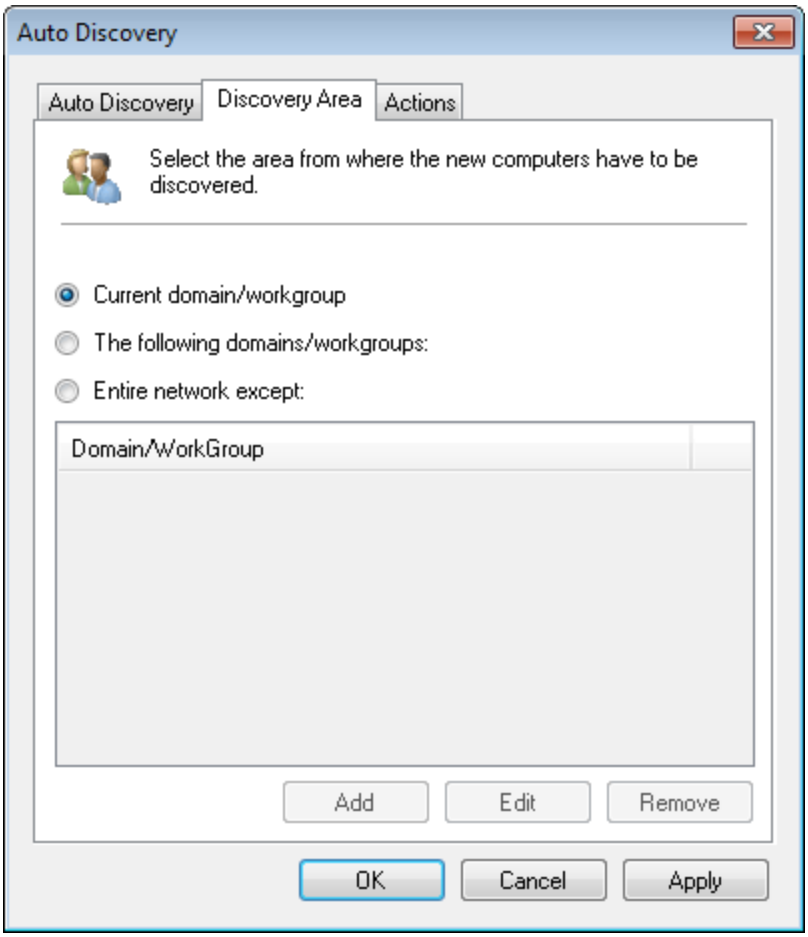
To configure the Auto Discovery settings:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Auto discovery settings…**.



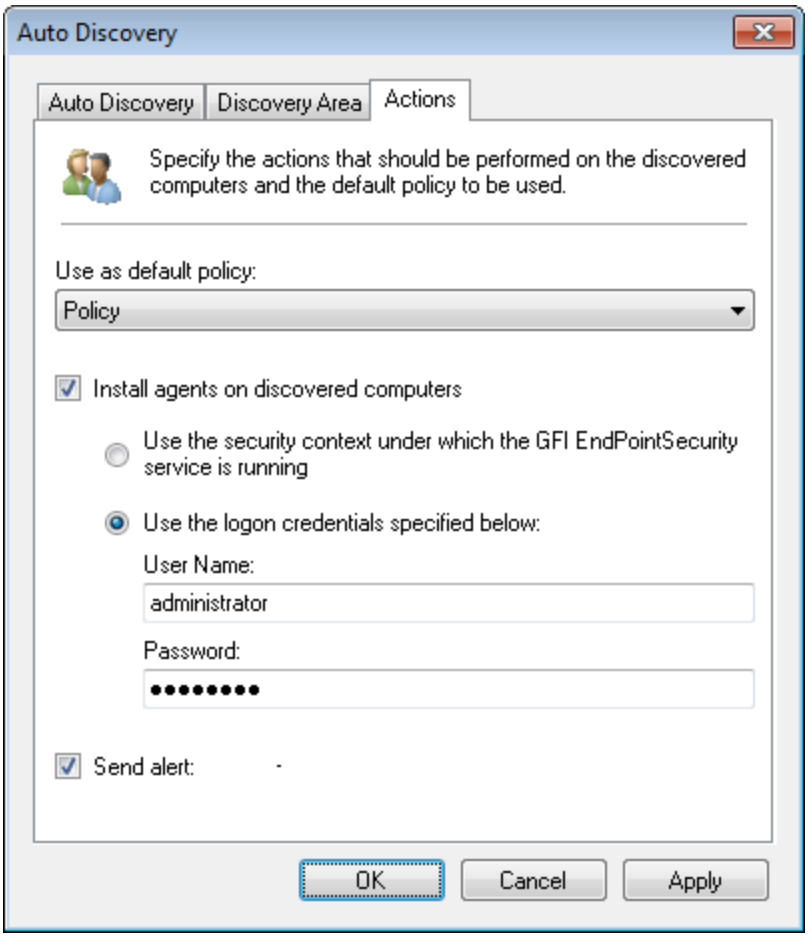
Screenshot 10: Auto Discovery options - Auto Discovery tab

3. Click **Start discovery now** to run auto discovery immediately.
4. Select/unselect **Enable automatic discovery to detect computers newly connected to the network**, to enable/disable Auto Discovery.
5. From the **Schedule** section select the start date and set frequency of the searches from Hourly, Daily, Weekly or Monthly.



Screenshot 11: Auto Discovery options - Discovery Area tab

6. Click **Discovery Area** tab and select the area to be covered by auto discovery. For **The following domains/workgroups** and **Entire network except**, click **Add** and key in the Domain/workgroup name.



Screenshot 12: Auto Discovery options - Actions tab

7. Click **Actions** tab and from the **Use as default policy** drop-down menu, select the policy you want to assign to newly discovered computers.
8. Select/unselect **Install agents on discovered computers** to enable/disable auto, agent deployment. Click **Yes** to confirm the enabling of Automatic Protection.
9. Select the logon mode that GFI EndPointSecurity uses to log on to the target computer(s) and deploy agents/protection policies. By default, GFI EndPointSecurity is configured to use the logon credentials of the currently logged-on user account from which GFI EndPointSecurity application is running.
10. Select/unselect **Send alert**, to enable/disable alerting options. For more information, refer to Configuring alerting options (page 129).
11. Click **Apply** and **OK**.

4.3 Configuring log on credentials

GFI EndPointSecurity requires to log on to the target computers in order to:

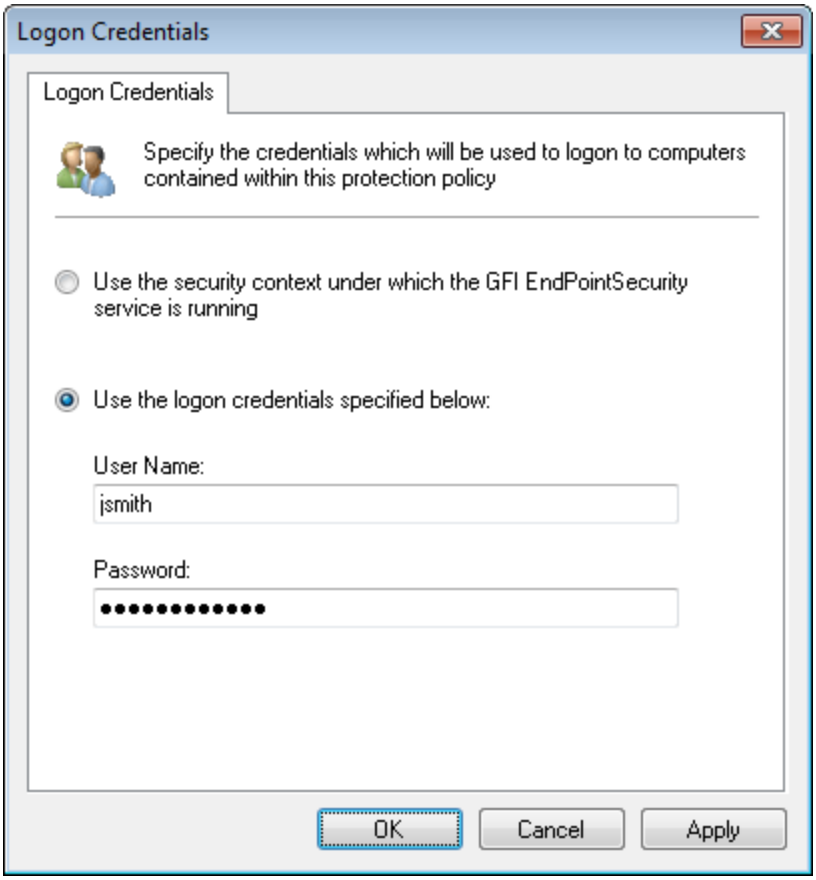
- Deploy agents and protection policy updates
- Keep track of the protection status of all target computers.

This requires that GFI EndPointSecurity is run under an account that has administrative privileges over your network target computers (example: a domain administrator account).

To specify logon credentials for a target computer:

1. Click **Configuration** tab > **Computers**.
2. Right-click on a computer from the list and click **Set logon credentials...**.

> **Note**
>
> If you want to set multiple computers to log on using the same credentials, highlight the required computers, right-click on one of them and click **Set logon credentials...**. Alternatively, click **Set logon credentials...** from **Actions**.



Screenshot 13: Logon Credentials dialog options

3. The table below describes the available logon credentials options:

Table 11: Logon credentials options

Option	Description
Use the security context under which GFI End-PointSecurity service is running	Use the same credentials that are running GFI End-PointSecurity.
Use the logon credentials specified below	Specify alternate credentials to use when logging in remote target computers. **Note** Specify credentials which have administrative privileges over scan targets.

4. Click **Apply** and **OK**.

Note

By default, GFI EndPointSecurity is configured to use the logon credentials of the currently logged-on user account, running GFI EndPointSecurity.

5 Managing Protection Policies

This chapter describes how to deploy newly created protection policies and schedule them. Prior to deployment you can also modify the settings of your protection policy.

Topics in this chapter

5.1 Creating a new protection policy 45

5.2 Assigning a Protection Policy 51

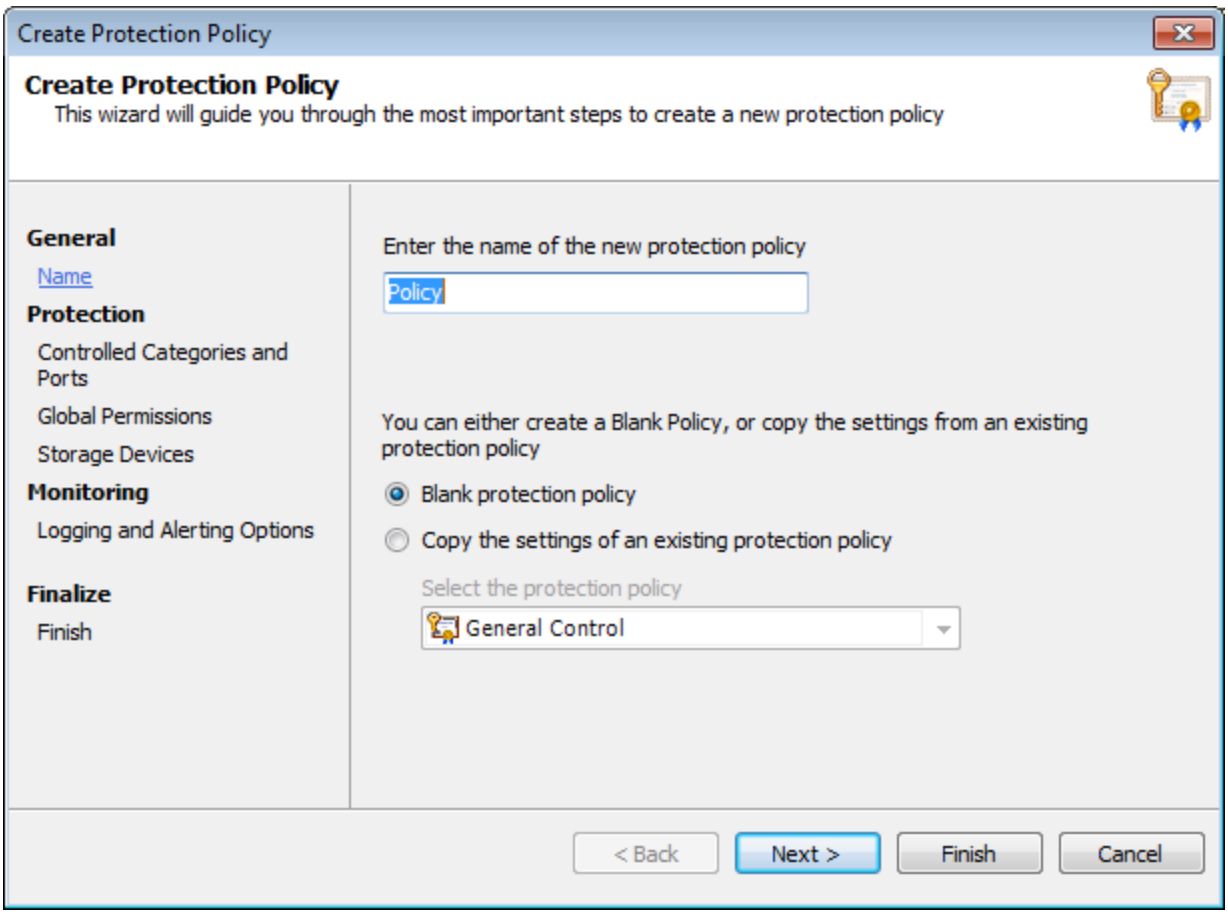
5.3 Verifying protection policy deployment 54

5.1 Creating a new protection policy

GFI EndPointSecurity ships with a default protection policy so that the software is operational upon installation. You can create further protection policies to suit your company's device access security policies.

To create a new protection policy:

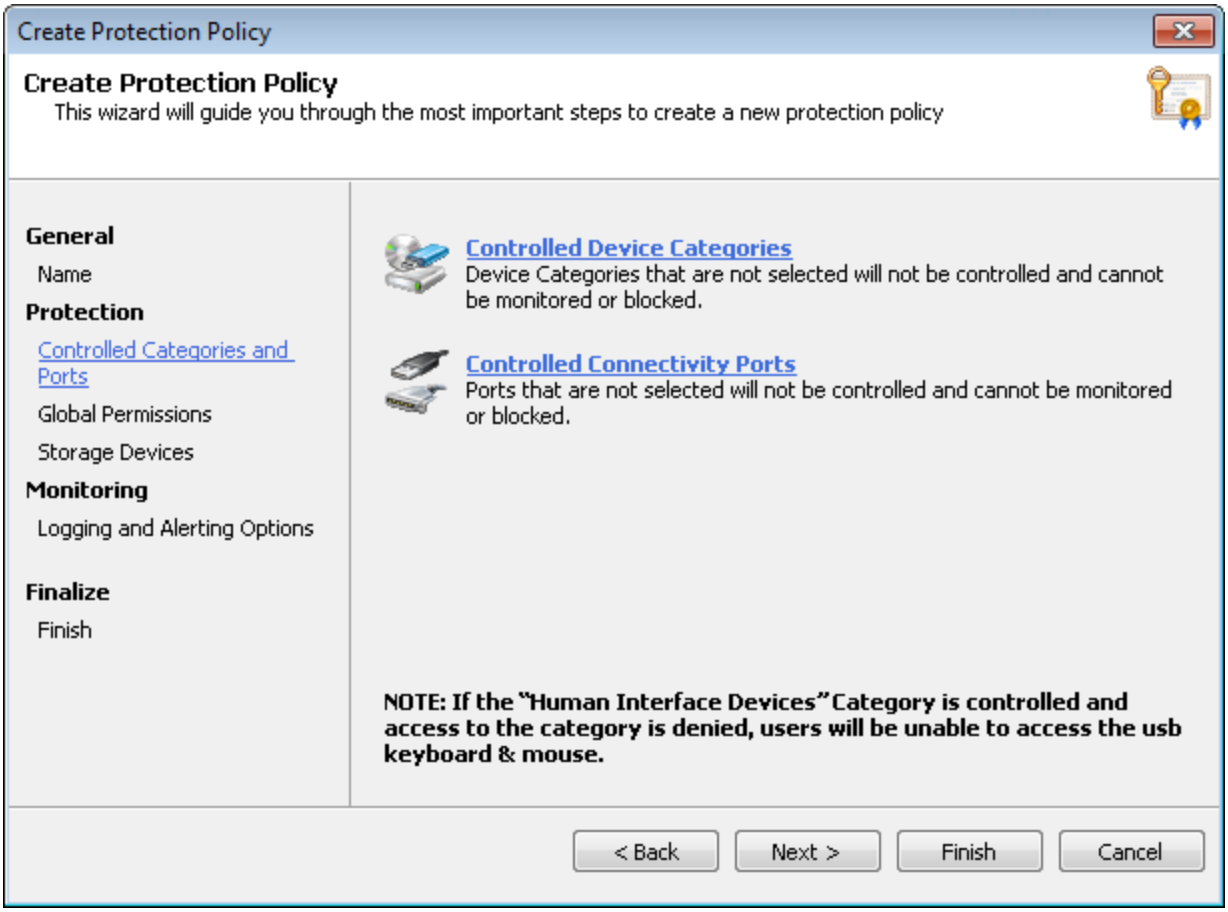
1. Click **Configuration** tab **> Protection Policies**.
2. From **Common tasks**, click **Create new protection policy…**.



Screenshot 14: Creating a new policy - General settings

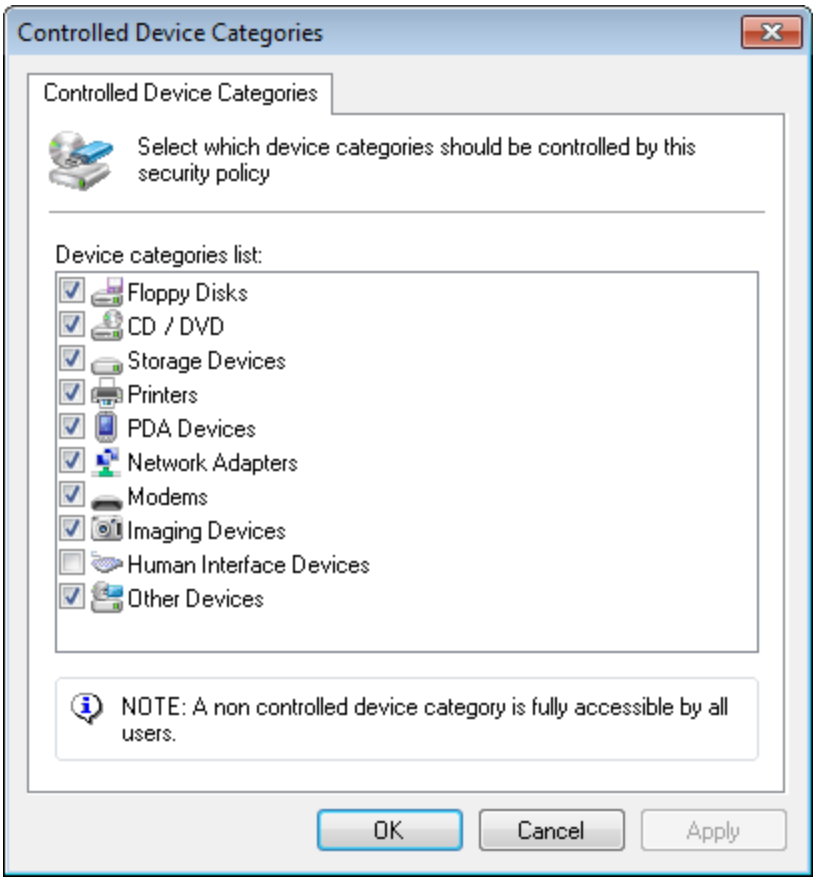
3. Key in a unique name for the new protection policy.

4. Select whether you want to create a blank policy or copy the settings from an existing policy. Click **Next**.In the settings area select the required settings inheritance option from:



Screenshot 15: Creating a new policy - Controlled Categories and Ports settings

5. Click **Controlled Device Categories**.

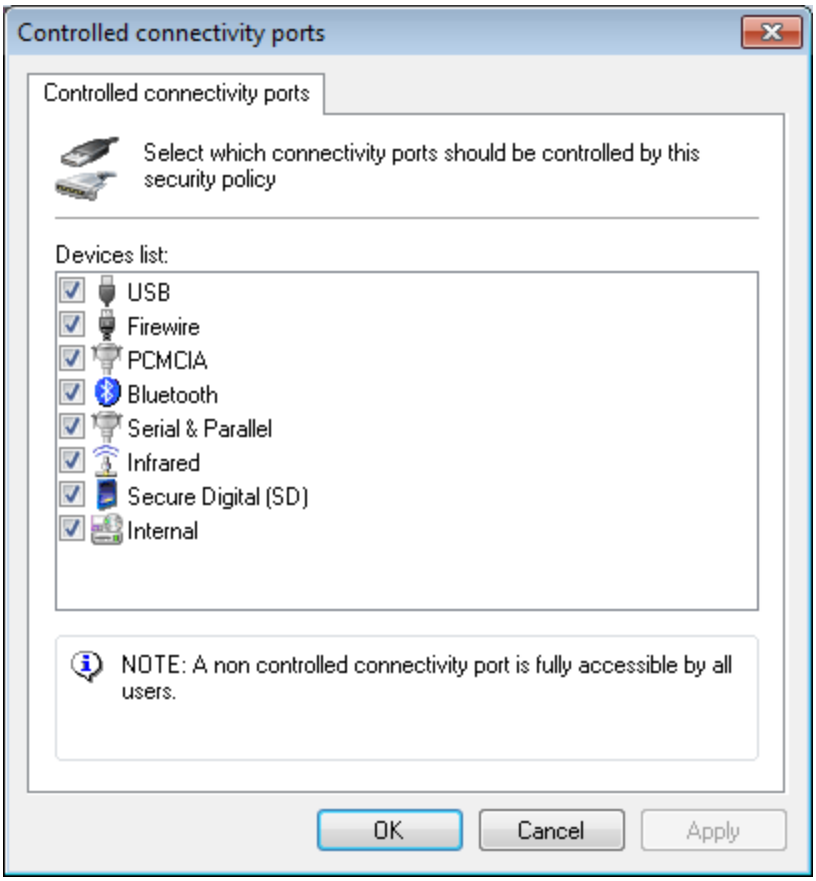


Screenshot 16: Controlled Device Categories options

6. From the **Controlled Device Categories** dialog, select the required device categories you want to control by this new policy. Click **OK** to close the **Controlled device categories** dialog and return to the wizard.

> **Important**
>
> If Human Interface Devices is enabled and access is denied, users will not be able to use USB keyboards and mice connected to target computers protected by this policy.

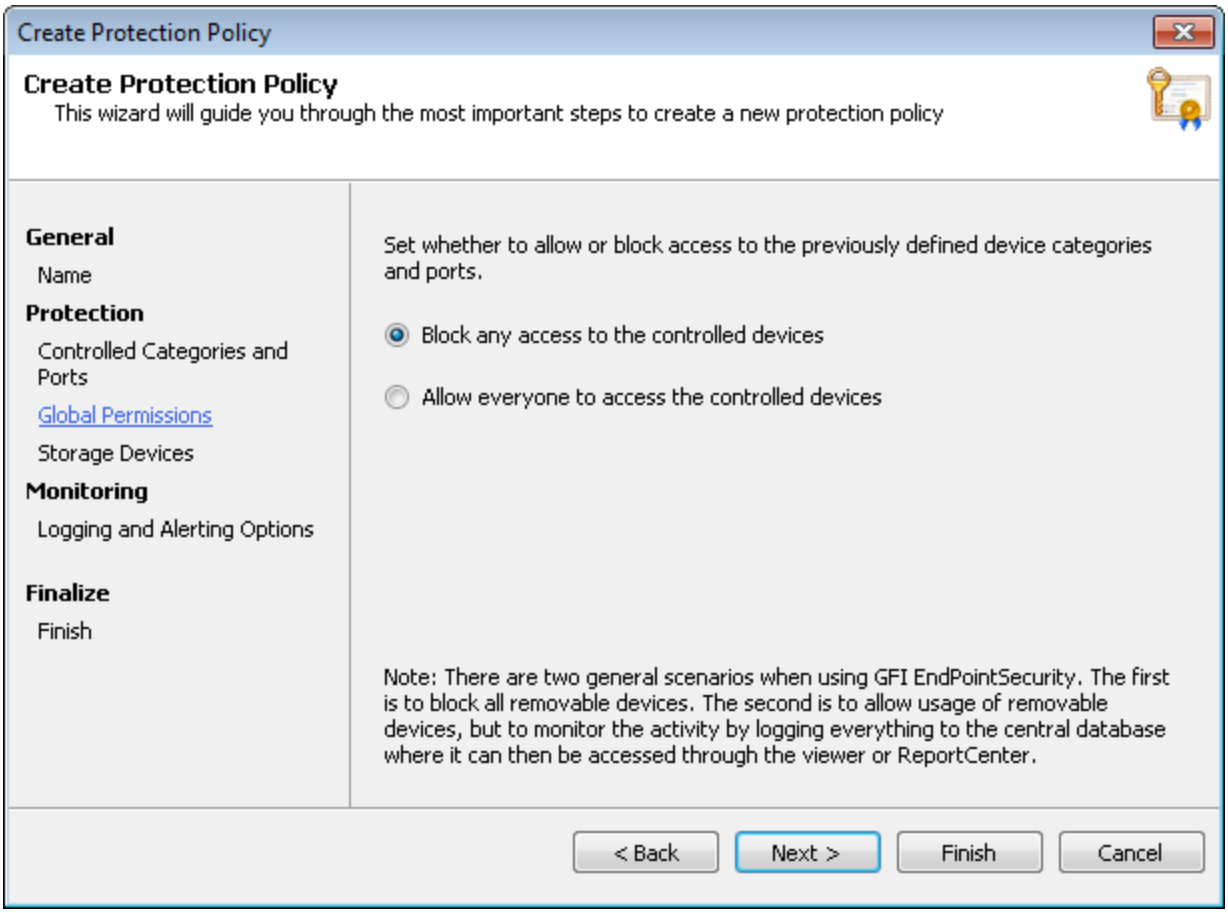
7. Click **Controlled Connectivity Ports**.



Screenshot 17: Controlled connectivity ports options

8. From the **Controlled connectivity ports** dialog, select the required connectivity ports that you want to control by this new policy. Click **OK** to close the **Controlled connectivity ports** dialog and return to the wizard.

9. Click **Next**.



Screenshot 18: Creating a new policy - Global Permissions settings

10. From the **Global Permissions** dialog, select the required global access permissions from:
    - **Block any access to the controlled devices** - to block access to all selected devices/ports.
    - **Allow everyone to access the controlled devices** - to allow access to all selected devices/ports. If this option is selected, activity monitoring will still be carried out on target computers covered by the protection policy.
11. Click **Next**.
12. Click **File-Type Filter** and add the file-types to block/allow by this policy.

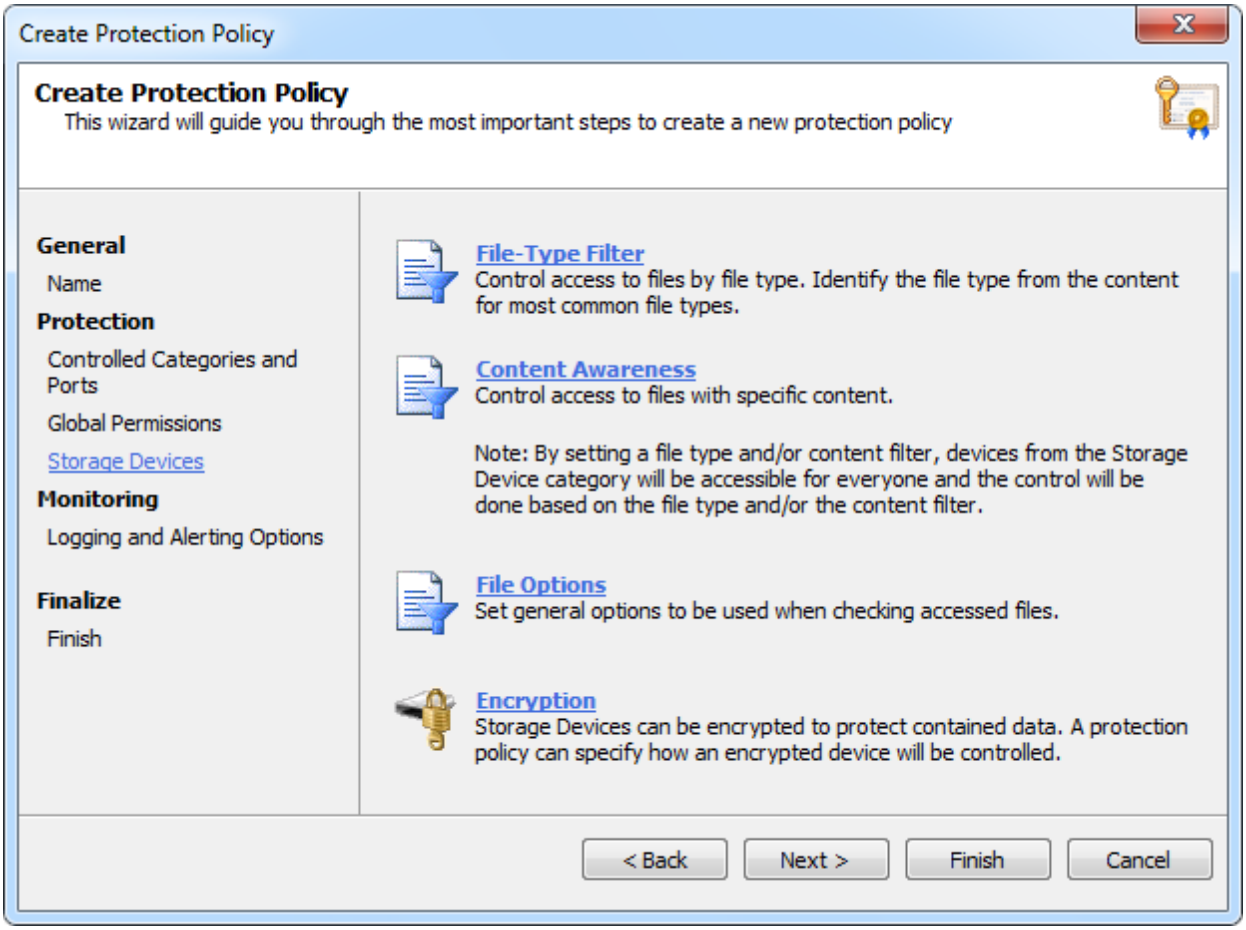
> **Note**
>
> GFI EndPointSecurity enables you to restrict access based on file-types. It is also able to identify the real content of most common file-types, (example: .DOC or .XLS files), and take the necessary actions applicable for the true file-type. This is most useful when file extensions are maliciously manipulated. For more information, refer to Configuring file-type filters (page 81).

13. Click **OK** to close the **File-Type Filter** dialog and return to the wizard.
14. Click **Encryption** and enable/configure the preferred encryption engine.

Note

In addition, GFI EndPointSecurity can also allow or block Active Directory (AD) users and/or user groups, from accessing specific file-types stored on devices that are encrypted with BitLocker To Go. These restrictions are applied when the encrypted devices are connected to the target computers covered by the protection policy. For more information, refer to Configuring security encryption (page 88).

15. Click **OK** to close the **Encryption** dialog and return to the wizard.
16. Click **Next**.



17. From **Storage Devices**, select the required options that you want to control from the tabs described below:

Table 12: Auto Discovery settings

Tab	Description
File-Type Filter	GFI EndPointSecurity enables you to specify file-type restrictions on files, such as .DOC or .XLS files, being copied to/from allowed devices. You can apply these restrictions to Active Directory (AD) users and/or user groups.

Tab	Description
Content Awareness	GFI EndPointSecurity enables you to specify the file content restrictions for a particular protection policy. The content awareness feature looks into files transiting the endpoints via removable devices and it \identifies content based on pre-configured and custom regular expressions and dictionary files. By default the module looks for secure confidential details such as social security numbers and primary account numbers as well as information related to companies and enterprises such as names of diseases, drugs, dangerous chemicals and also trivial language or ethnic / racist terms. » You can configure content checking as a global policy in a similar fashion to the file checking module.
File Options	GFI EndPointSecurityenables you to specify the options required to block or allow files based on size. GFI EndPointSecurity also enables you to ignore large files when checking file type and content and archived files.
Encryption	GFI EndPointSecurity enables you to configure settings that specifically cater for encrypted devices. It also enables you to encrypt devices that are not yet secured.

Note

For more information refer to For more information, refer to Customizing Protection Policies (page 57).

18. Configure logging and alerting options for this policy and click **Next**.

Note

For more information, refer to Configuring event logging and Configuring alerts.

19. Review the summary page for information about your policy and click **Finish**.

5.2 Assigning a Protection Policy

The next step is to link the relevant set of device access and connectivity port permissions to each target computer. You can do this by assigning protection policies to target computers.

Note

Target computers can only be assigned one protection policy at a time.

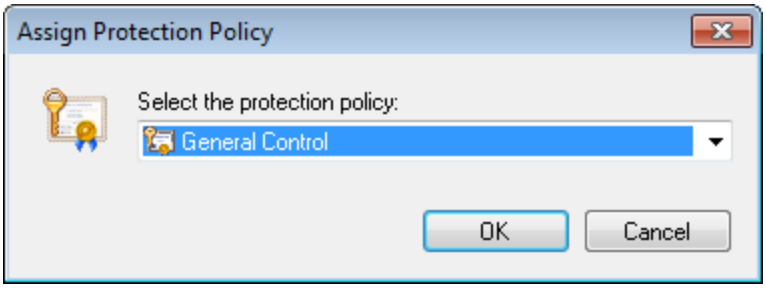
To assign a protection policy on to a target computer:

1. From the GFI EndPointSecurity management console, select **Configuration**.
2. Click **Computers**.
3. Highlight the required target computer(s).

Note

If assigning the same policy to more than one target computer, select all the required target computers and then specify the protection policy for the selected set of target computers.

4. From the left pane, click the **Assign Protection Policy**hyperlink in the **Actions** section.



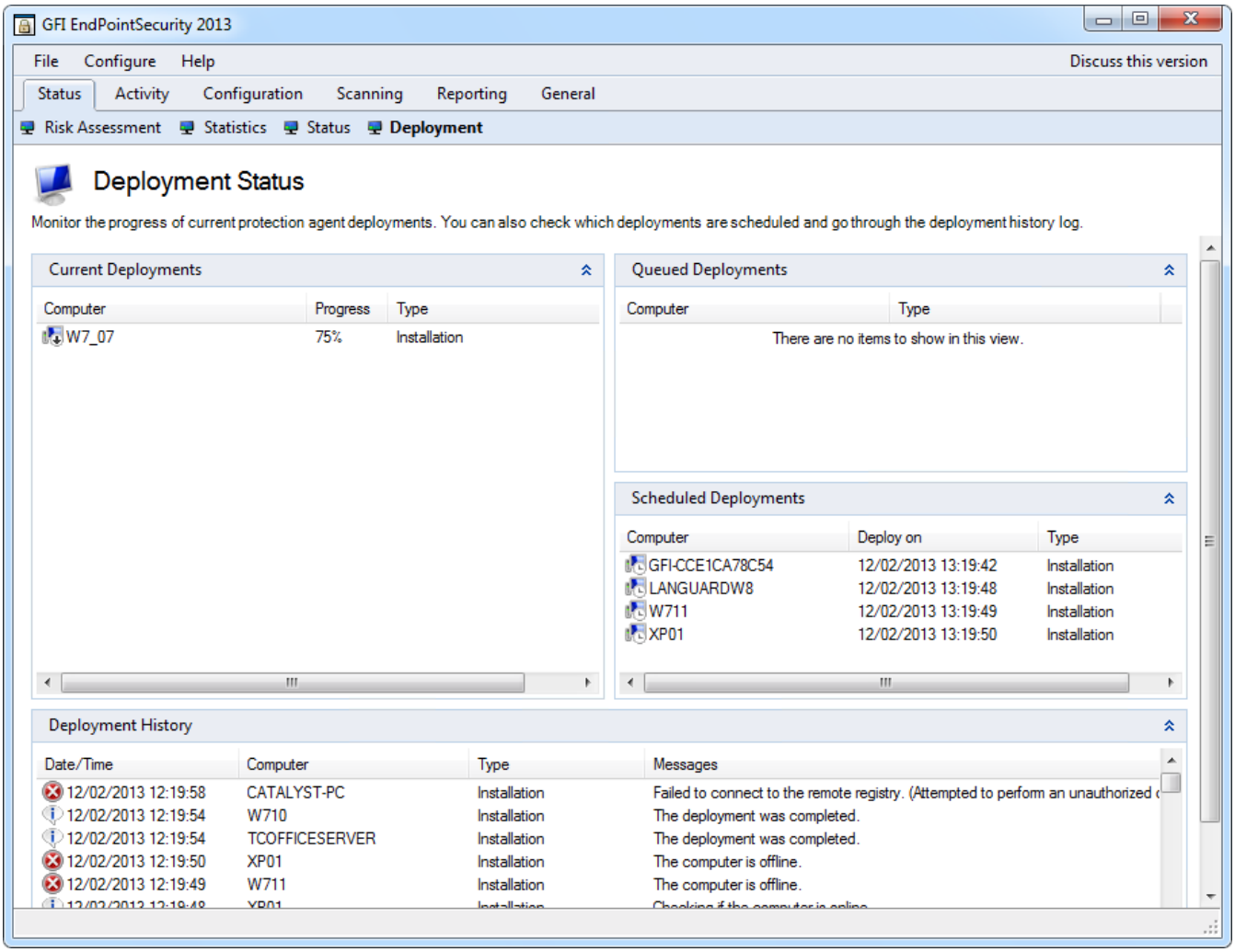
Screenshot 19: Assign Protection Policy Options

5. In the **Assign Protection Policy** dialog select the required protection policy from the drop down list, and click **OK**.

5.2.1 Deploy immediately

To immediately deploy a protection policy on target computers:

1. Click **Configuration** tab **>** **Computers** sub-tab.
2. Highlight the required target computer(s). If more than one deployment is required, you can highlight all the required target computers at once and then deploy the protection policies to the selected set of target computers.
3. From **Actions**, click **Deploy now…**. The view should automatically change to **Status > Deployment**.

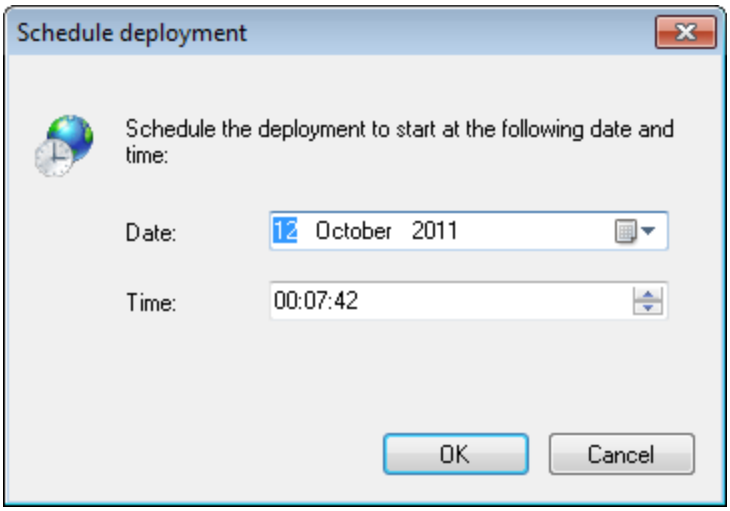


Screenshot 20: Deploying a policy immediately - Deployment sub-tab

5.2.2 Scheduled policy deployment

To schedule deployment of a protection policy:

1. Click **Configuration** tab **> Computers.**
2. Highlight the required target computer(s). If more than one deployment is required, you can highlight all the required target computers at once and then deploy the policies to the selected set of target computers.
3. From **Actions**, click **Schedule deployment….**



Screenshot 21: Schedule deployment options

4. From **Schedule deployment** dialog select the deployment date and time, and click **OK**.

> **Note**
>
> If the target computer is offline, the deployment of the relevant policy is rescheduled for an hour later. GFI EndPointSecuritykeeps trying to deploy that policy every hour, until the target computer is back online.

5.2.3 Deploying policies through Active Directory

You can create a Windows installer package (.msi installation file) that you can then deploy through Active Directory Group Policies across target computers in your domain.

To create the Windows installer package:

1. Click **Configuration** tab **> Protection Policies**.
2. From the left pane, select the protection policy for which you want to create the Windows installer package.
3. From the right pane, click **Deploy through Active Directory** in the **Deployment** section.
4. Key in the **File name** of the .msi file and browse to select the destination path.
5. Click **Save**.

> **Note**
>
> For information on how to deploy software using Active Directory Group Policies in Microsoft Windows Server 2003 and Microsoft Windows Server 2008, refer to http://support.microsoft.com/kb/816102

5.3 Verifying protection policy deployment

Once a protection policy is deployed, it is recommended to verify that target computers were affected by the policy. Verify if the deployment was successful from:

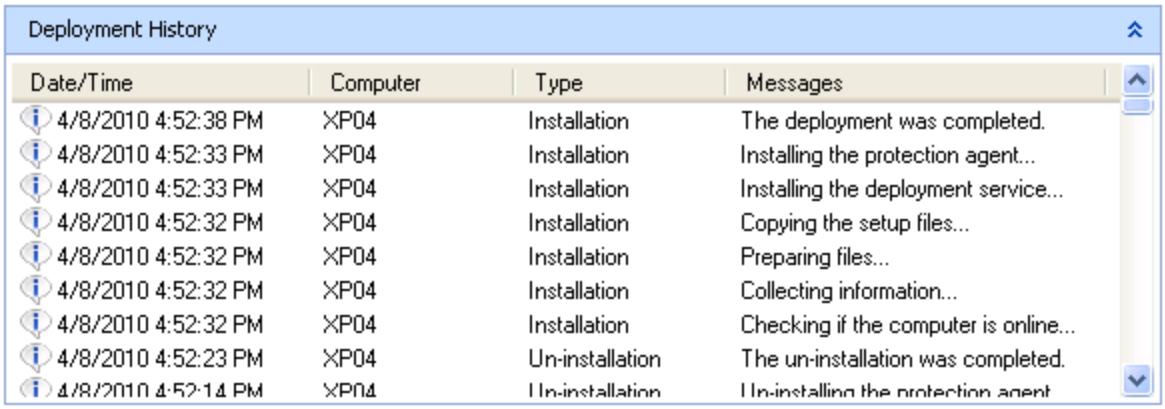
- Deployment history area
- Agents' status area

5.3.1 Deployment History

Use the information displayed in the Deployment History area to determine whether deployment for each target computer completed successfully, or whether errors were encountered.

To view the deployment history:

1. Click **Status> Deployment**.



Screenshot 22: Deployment History area

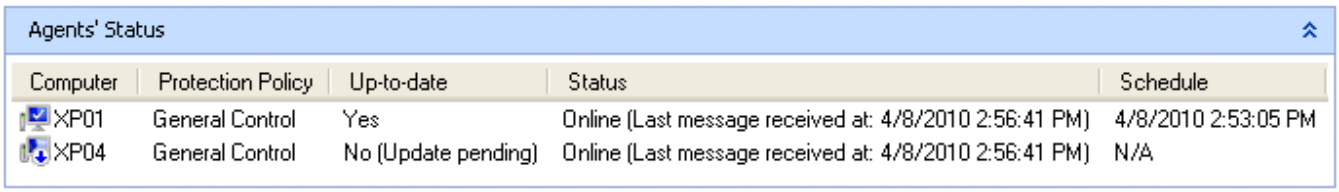
2. From **Deployment History**, confirm the successful completion of the update onto the local computer. For more information, refer to Deployment status view (page 119).

5.3.2 Agents' status

Use the information displayed in the Agents' Status area to determine the status of all deployment operations performed on your network target computers.

To view agents' status:

3. Click **Status> Agents**.



Screenshot 23: Agent's Status area

4. From **Agents' Status**, confirm the successful assignment of the correct protection policy to the target computer(s) and that agent deployment is up-to-date.

> **Note**
>
> Each agent sends its online status to the main GFI EndPointSecurity installation at regular intervals. If this data is not received by the main installation, the agent is considered to be offline.

Note

If a target computer is offline, the deployment of the relevant policy is rescheduled for an hour later. GFI EndPointSecurity keeps trying to deploy that policy every hour, until the target computer is back online.

For more information about the agents status area, refer to the Agents status view section in the Monitoring statuses chapter.

6 Customizing Protection Policies

This chapter provides you with information related to modifying the settings of your pre-configured protection policies. This enables you to tweak settings by time, as you discover new security obstacles and possible vulnerabilities.

Topics in this chapter

6.1 Configuring controlled device categories 57

6.2 Configuring controlled connectivity ports 58

6.3 Configuring power users 59

6.4 Configuring access permissions for device categories 60

6.5 Configuring access permissions for connectivity ports 63

6.6 Configuring access permissions for specific devices 65

6.7 Viewing access permissions 68

6.8 Configuring priorities for permissions 70

6.9 Configuring device blacklist 70

6.10 Configuring device whitelist 74

6.11 Configuring temporary access privileges 77

6.12 Configuring file-type filters 81

6.13 Configuring content awareness 83

6.14 Configuring file options 86

6.15 Configuring security encryption 88

6.16 Configuring event logging 94

6.17 Configuring alerts 96

6.18 Setting a policy as the default policy 99

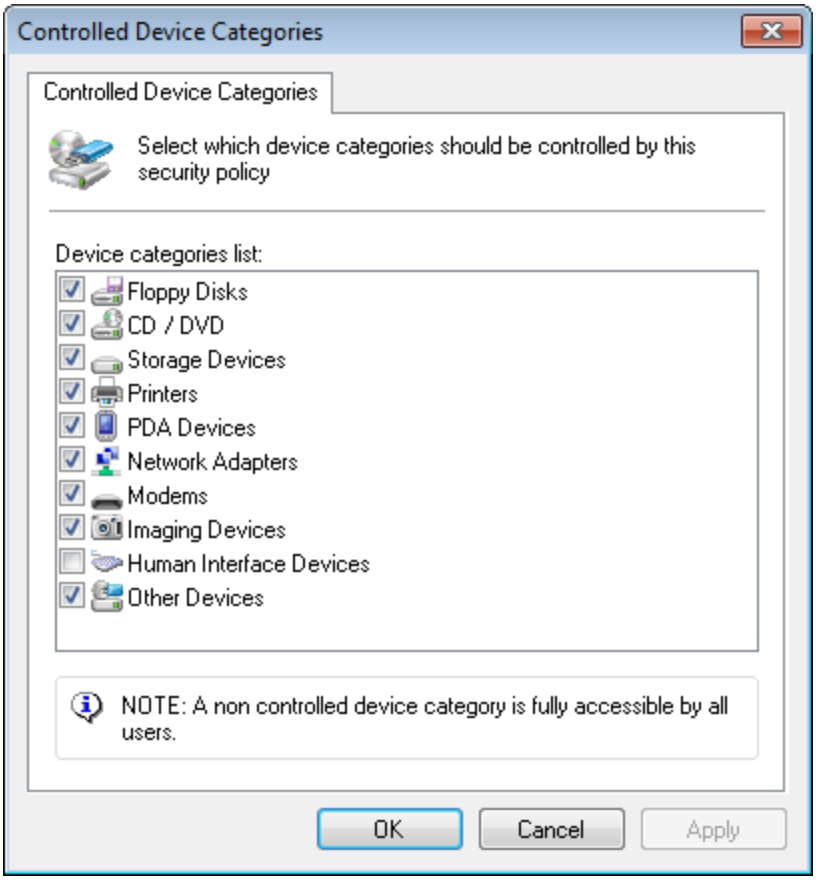
6.1 Configuring controlled device categories

GFI EndPointSecurity enables you to select which supported device categories should be controlled or not by a protection policy. You can do this on a policy-by-policy basis.

> **Note**
>
> Unspecified devices will be fully accessible from the target computers covered by the protection policy. As a result, GFI EndPointSecurity cannot monitor and block devices falling in a category that is not controlled by the protection policy.

To configure devices controlled by a protection policy:

1. Click **Configuration** tab > **Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. Click **Security**.
4. From **Common tasks**, click **Edit controlled device categories…**.



Screenshot 24: Controlled Device Categories options

5. From the **Controlled Device Categories** dialog, select/unselect the required device categories that will be controlled by the protection policy, and click **OK**.

Important

If you enable Human Interface Devices and deny access such devices, users will not be able to use USB keyboards and mice connected to target computers protected by this policy.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers…**.

6.2 Configuring controlled connectivity ports

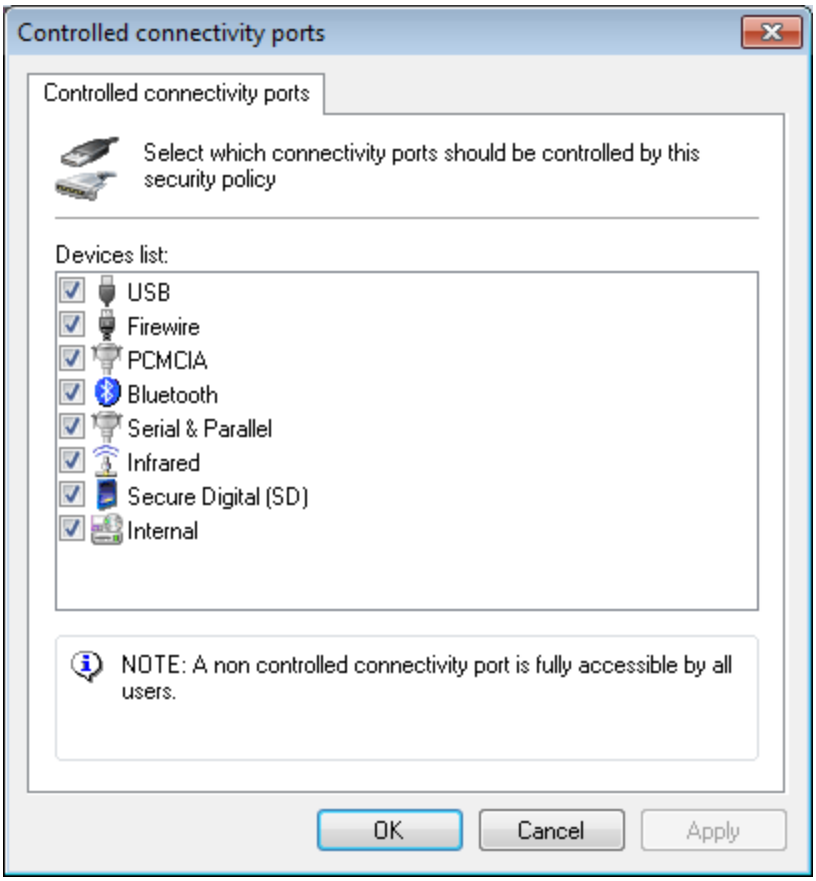
GFI EndPointSecurity enables you to select which supported connectivity ports should be controlled or not by a protection policy. You can do this on a policy-by-policy basis.

Note

Unspecified ports will be fully accessible from the target computers covered by the protection policy. As a result, GFI EndPointSecurity cannot monitor and block devices connected to a port that is not controlled by the protection policy.

To configure which ports will be controlled by a specific protection policy:

1. Click **Configuration** tab **> Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. Click **Security**.
4. From **Common tasks**, click **Edit controlled ports…**.



Screenshot 25: Controlled connectivity ports options

5. From the **Controlled connectivity ports** dialog, select/unselect the required connectivity ports that will be controlled by the protection policy, and click **OK**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers…**.

6.3 Configuring power users

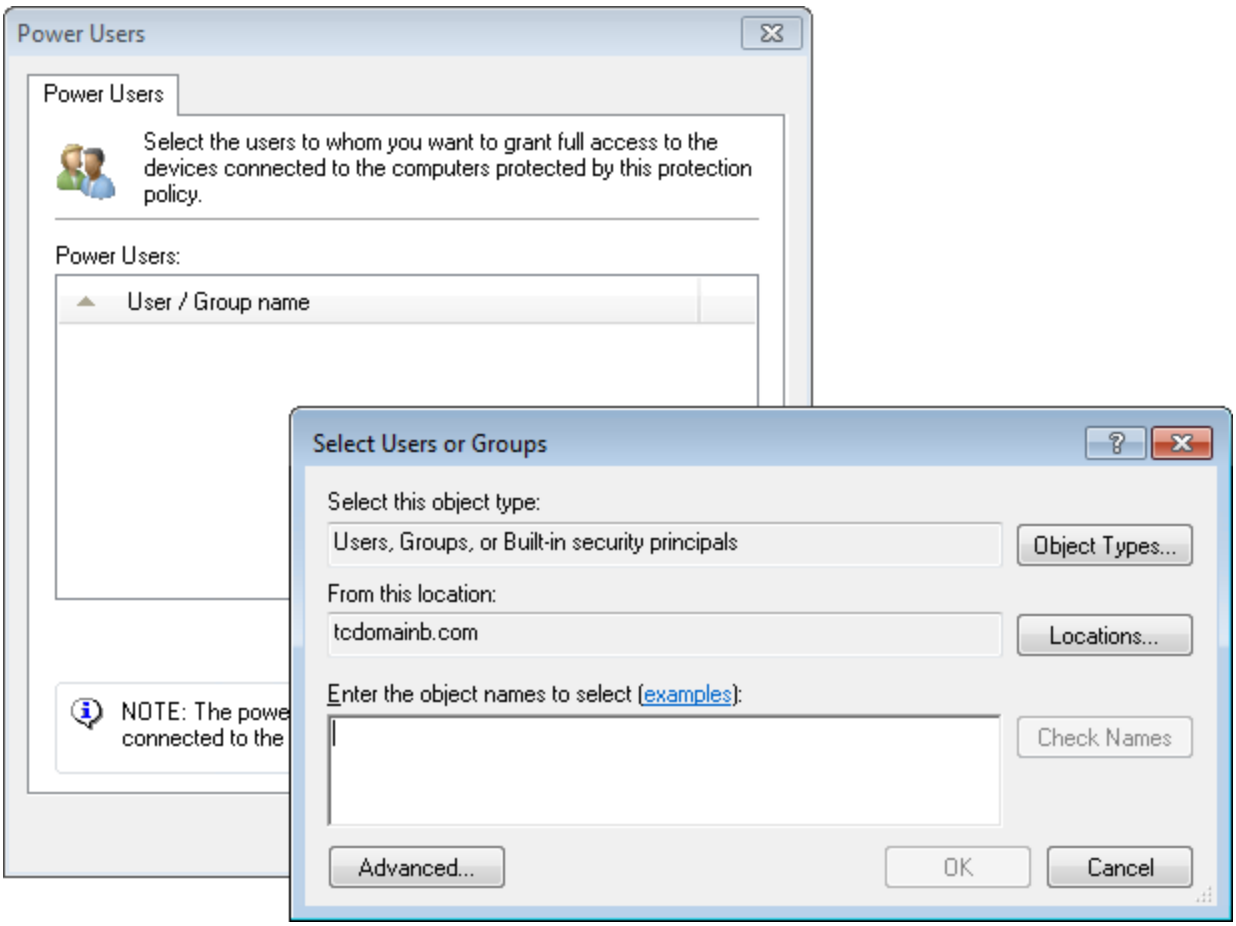
GFI EndPointSecurity enable you to specify Active Directory (AD) users and/or user groups, as power users. Power users are automatically given full access to devices connected to any target computer

covered by a protection policy. You can define sets of power users on a policy-by-policy basis.

You should exercise caution when using this feature, since incorrectly specifying a user as a power user will lead to that user overriding all restrictions of the relevant protection policy.

To specify power users of a protection policy:

1. Click **Configuration** tab **> Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. From the right pane, click **Power users** in the **Security** section.



Screenshot 26: Power users options

4. In the Power Users dialog:

» **Option 1**: Click **Add…** to specify the user(s)/group(s) that will be set as power users for this protection policy, and click **OK**.

» **Option 2**: Highlight user(s)/group(s) and click **Remove** to demote from power users, and click **OK**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers…**.

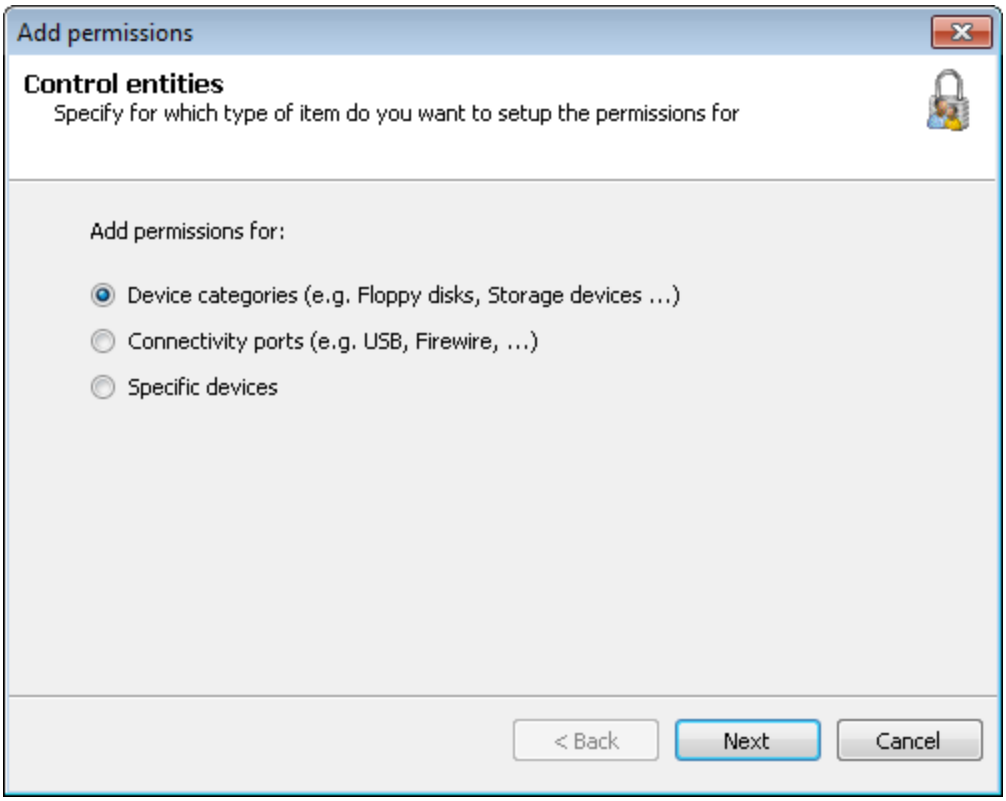
6.4 Configuring access permissions for device categories

GFI EndPointSecurity enables you to set permissions by device categories to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis.

When a device category is not set to be controlled by the particular security policy, the relevant entry is disabled. For more information, refer to Configuring controlled device categories (page 57).

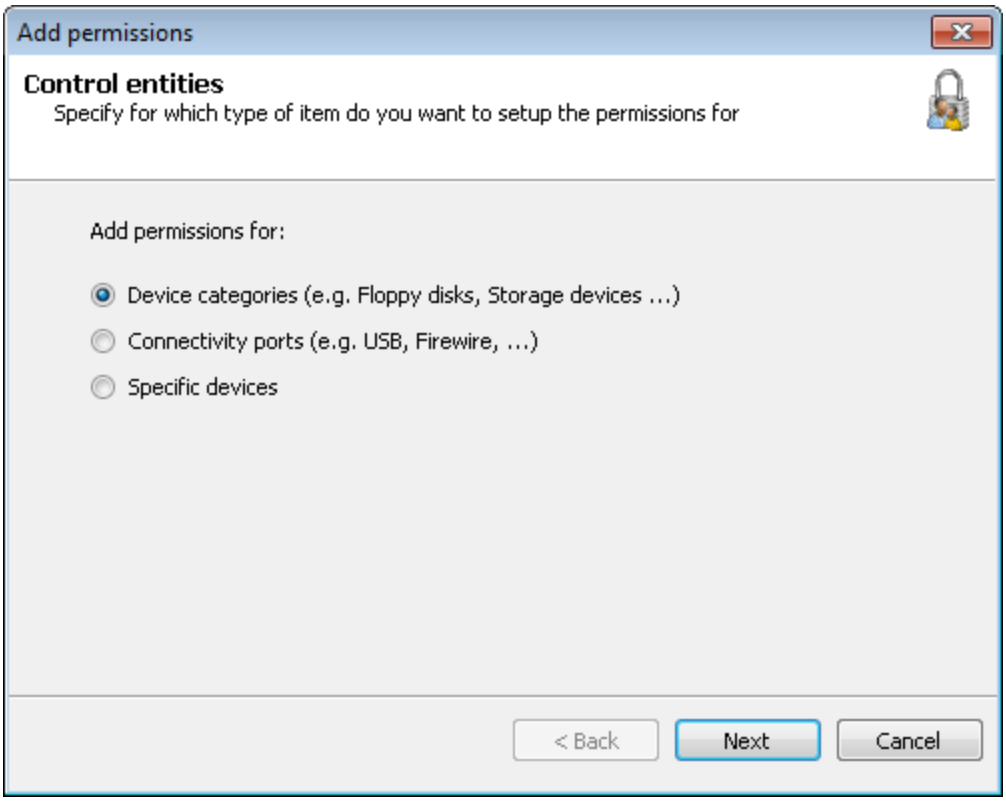
To configure device category access permissions for users in a protection policy:

1. Click **Configuration** tab > **Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. From **Common tasks**, click **Add permission(s)...**.



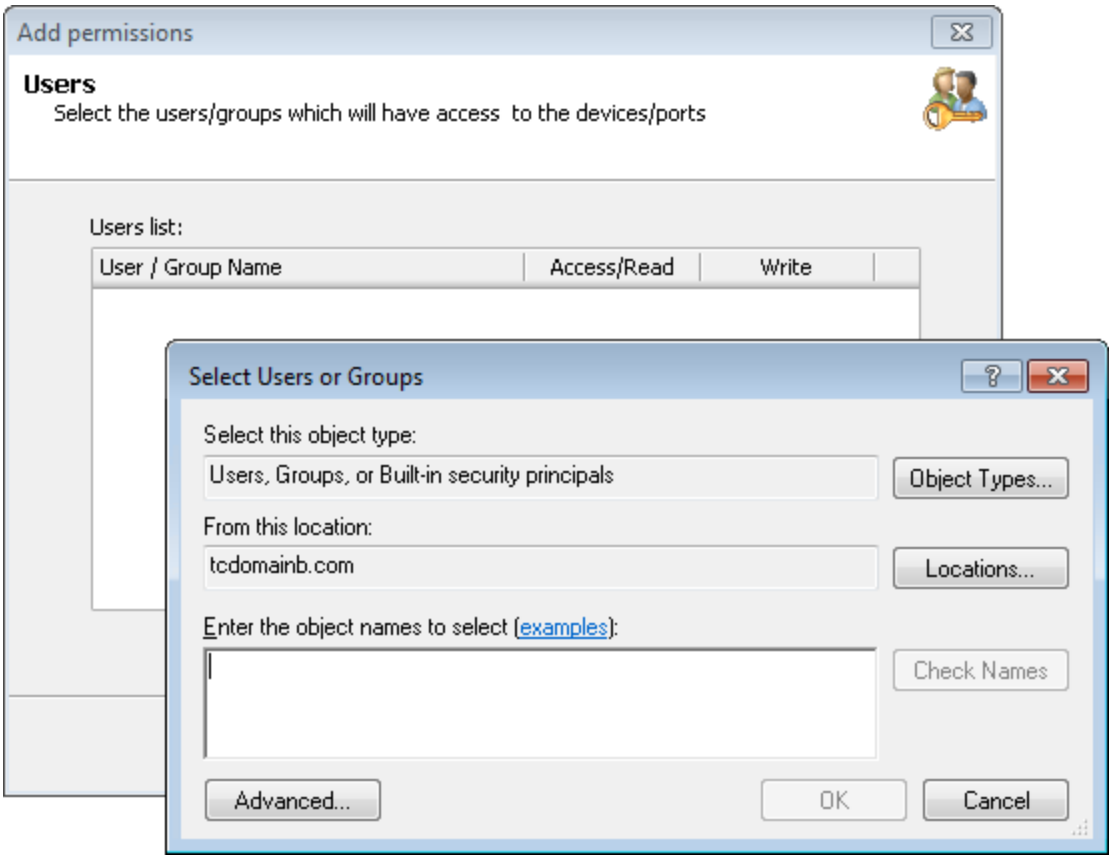
Screenshot 27: Add permissions options - Control entities

4. In the **Add permissions** dialog select **Device categories** and click **Next**.



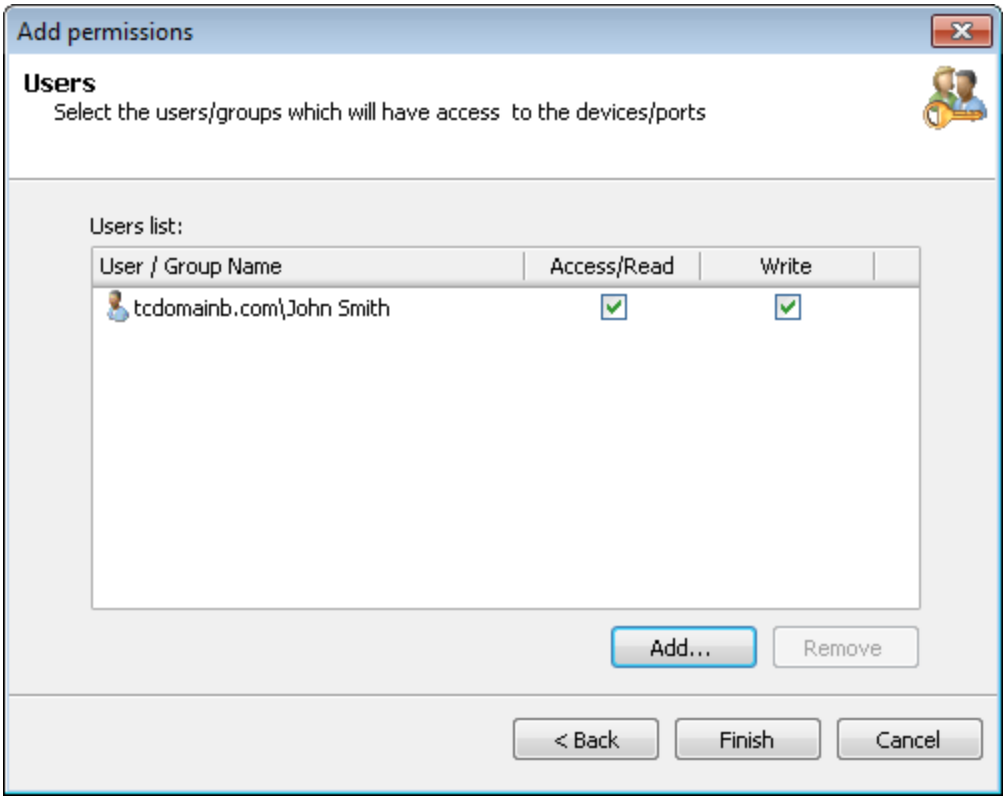
Screenshot 28: Add permissions options - Device categories

5. Enable or disable the required device categories for which to configure permissions, and click **Next**.



Screenshot 29: Add permissions options - Users

6. Click **Add…** to specify the user(s)/group(s) that will have access to the device categories specified in this protection policy, and click **OK**.



Screenshot 30: Add permissions options - Users

7. Enable or disable Access/Read and Write permissions for each user/group you specified and click **Finish**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers…**.

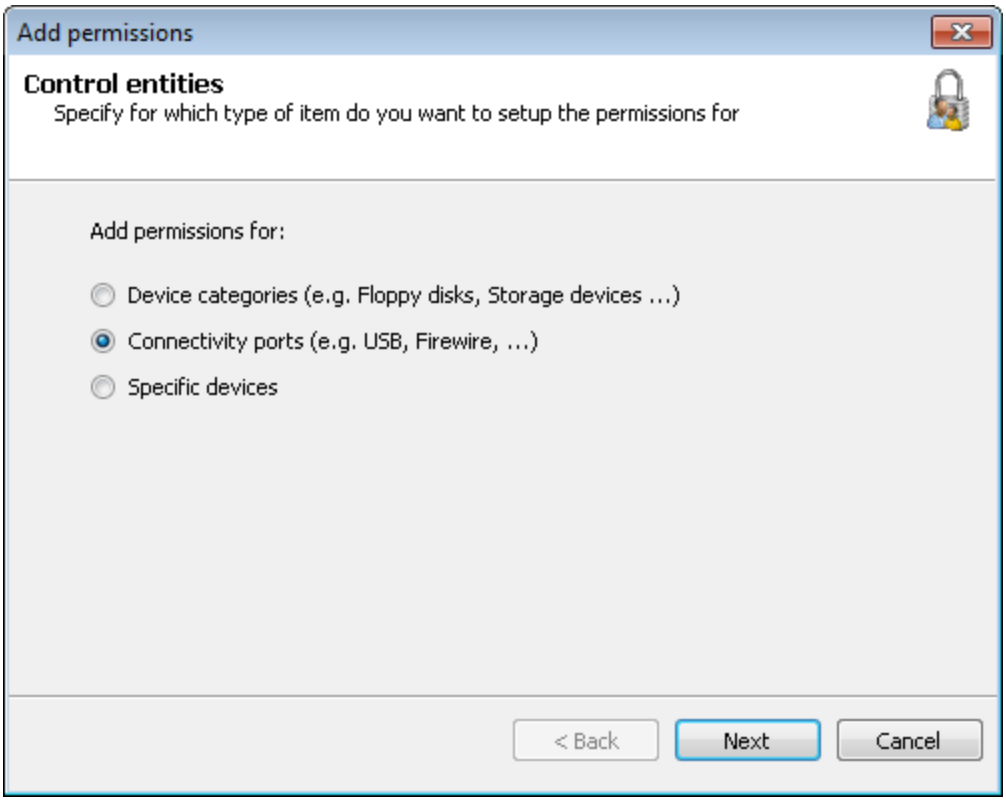
6.5 Configuring access permissions for connectivity ports

GFI EndPointSecurity provides you with the facility to set permissions by connectivity ports to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis.

When a connectivity port is not set to be controlled by a protection policy, the relevant permission is disabled. For more information, refer to Configuring controlled connectivity ports (page 58).

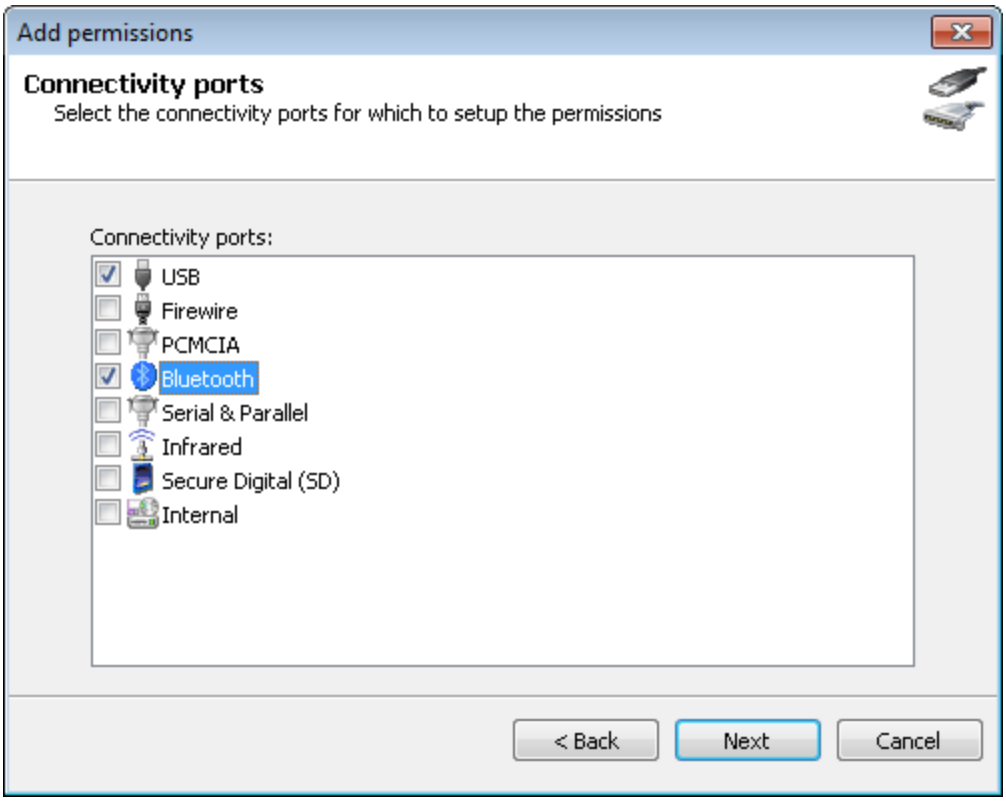
To configure connectivity port usage permissions for users within a specific protection policy:

1. Click **Configuration** tab **> Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. Click **Security** > **Set Permissions**
4. From **Common tasks**, click **Add permission(s)…**.



Screenshot 31: Add permissions options - Control entities

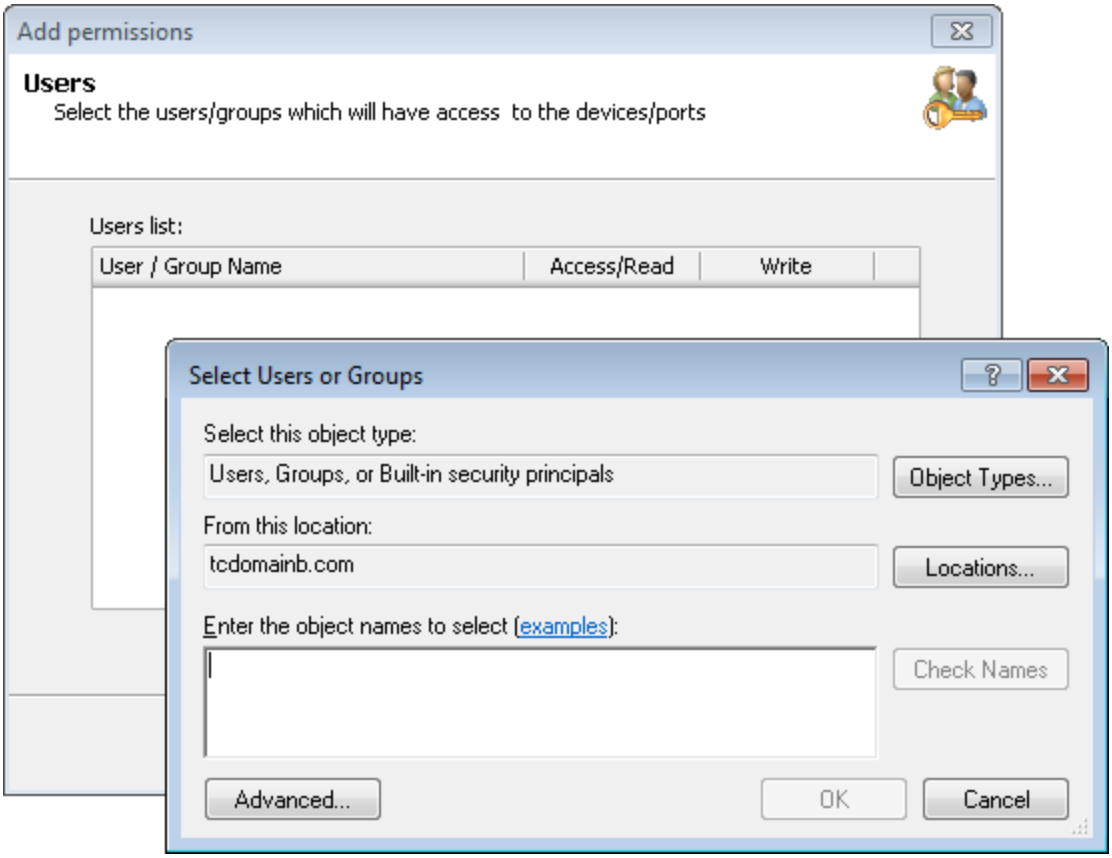
5. In the **Add permissions** dialog select **Connectivity ports** and click **Next**.



Screenshot 32: Add permissions options - Connectivity ports

6. Enable or disable the required connectivity ports for which to configure permissions, and click **Next**.

7. Click **Add…** to specify the user(s)/group(s) that will have access to the connectivity ports specified in this protection policy, and click **OK**.



Screenshot 33: Add permissions options - Users

8. Enable or disable Access/Read permissions for each user/group you specified, and click **Finish**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers…**.

6.6 Configuring access permissions for specific devices

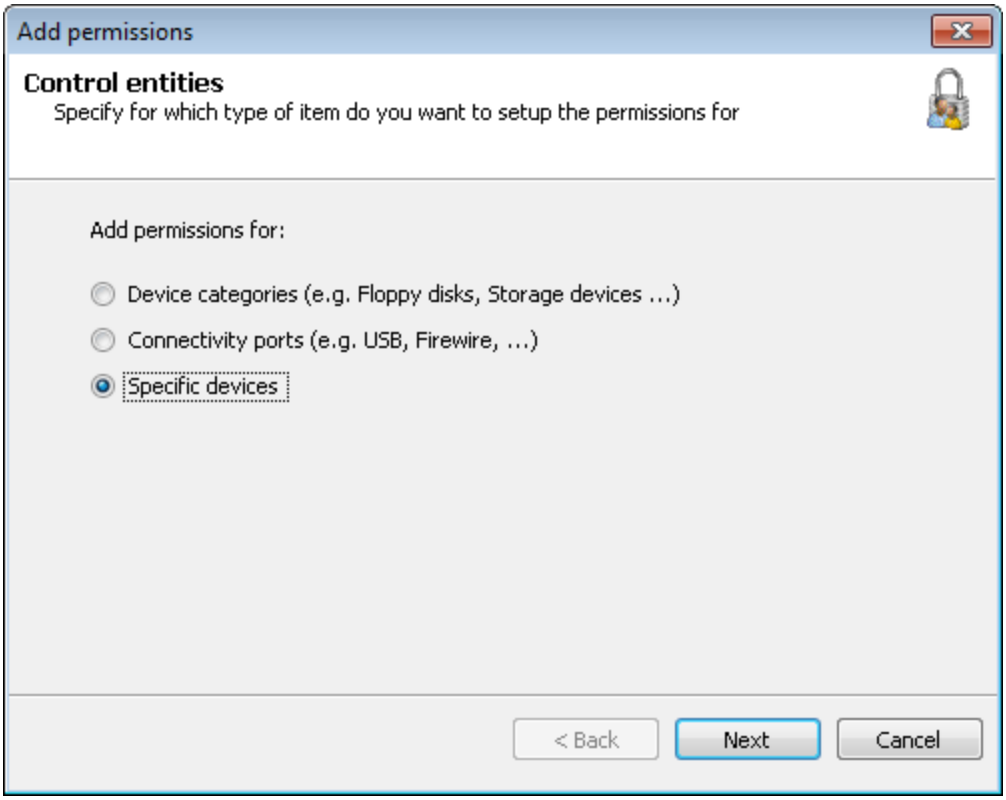
GFI EndPointSecurity enables you to set permissions by specific devices to Active Directory (AD) users and/or user groups. You can do this on a policy by policy basis.

For example, you can assign read-only permissions to a specific company approved USB pen drive. Attempts to use any other non-approved USB pen drives will be blocked.

> **Note**
>
> For an updated list of devices currently connected to the target computers, run a device scan and add the discovered devices to the devices database prior to configuring access permissions for specific devices. For more information, refer to Discovering Devices (page 100).

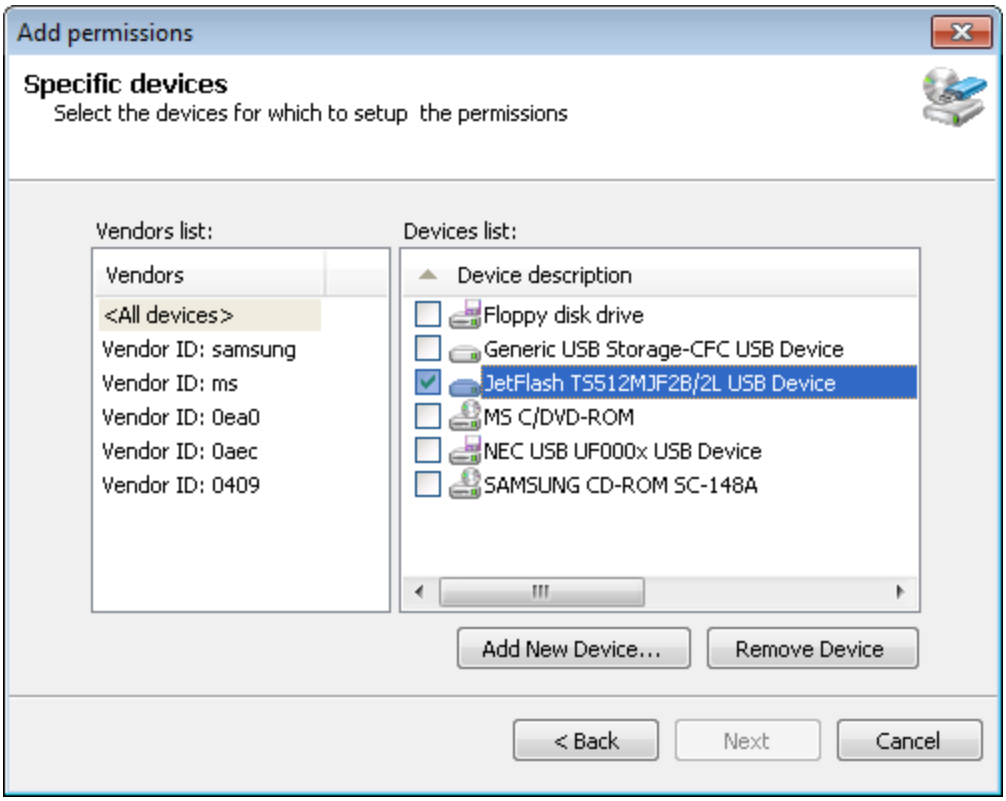
To configure specific device access permissions for users in a protection policy:

1. Click **Configuration** tab > **Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. Click **Security** sub-node.
4. From the left pane, click **Add permission(s)…**in the **Common tasks** section.



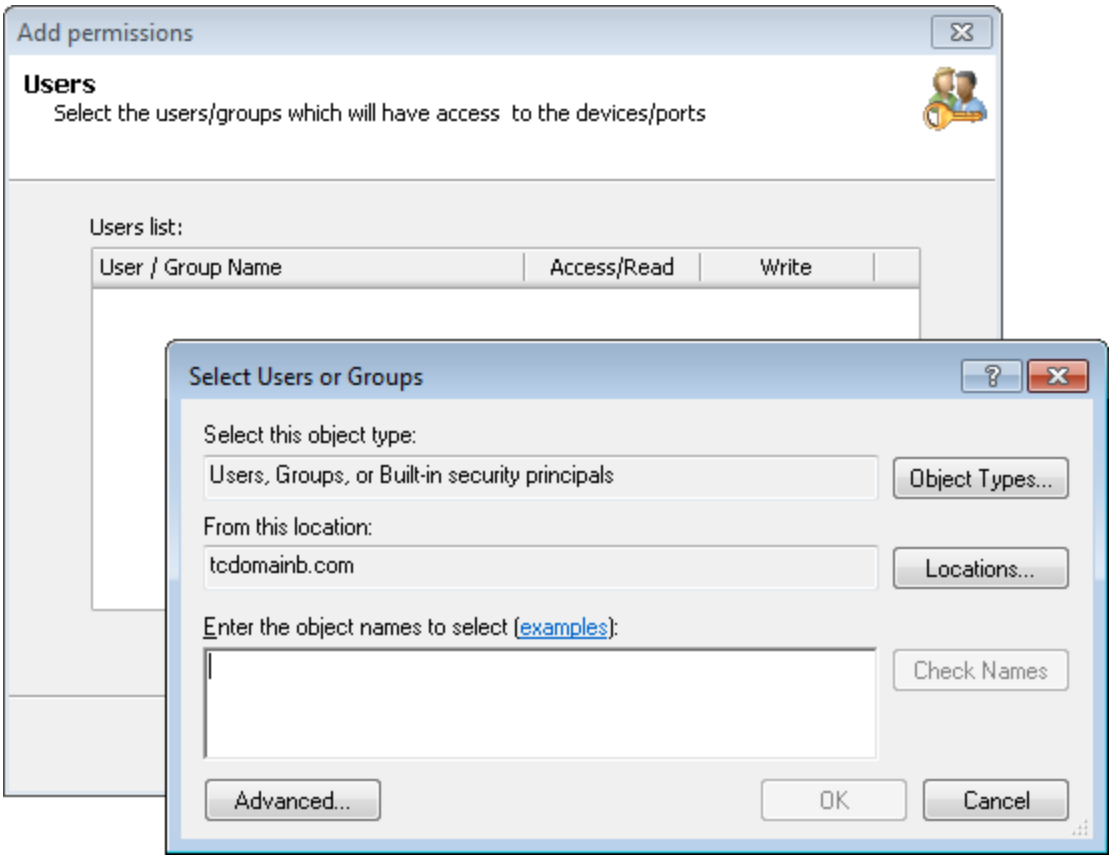
Screenshot 34: Add permissions options - Control entities

5. In the **Add permissions** dialog select **Specific devices** and click **Next**.



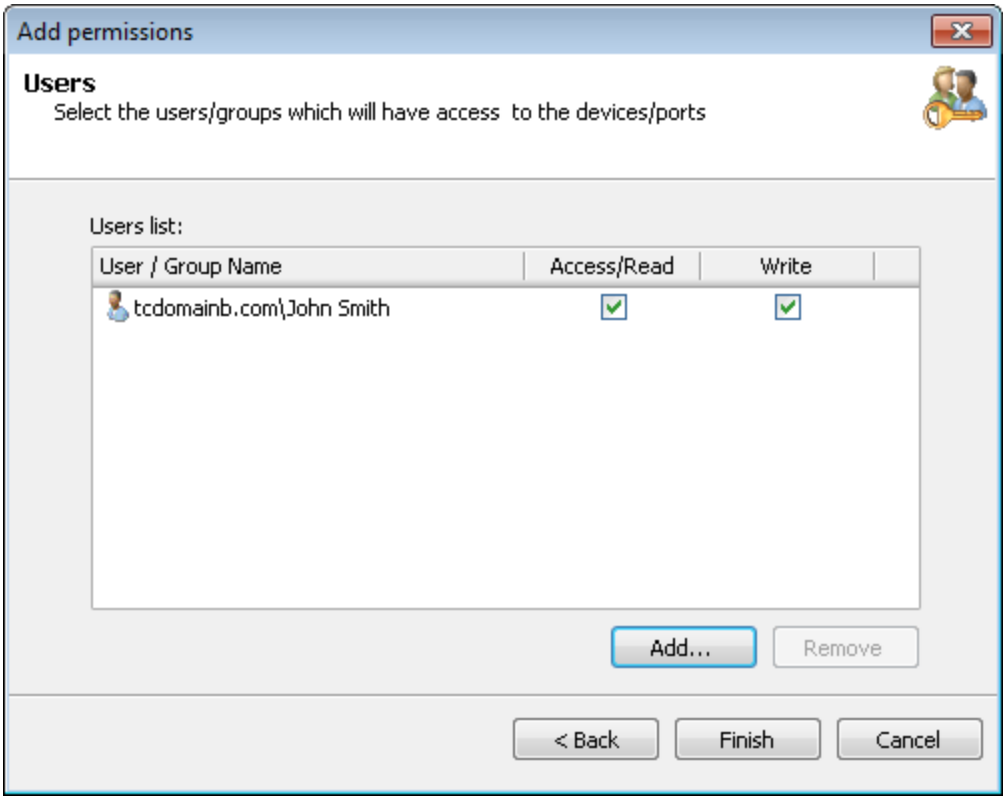
Screenshot 35: Add permissions options - Specific devices

6. Enable or disable the required devices from the Devices list, for which to configure permissions, and click **Next**. If a required device is not listed, click **Add New Device…** to specify the details of the device for which to configure permissions, and click **OK**.



Screenshot 36: Add permissions options - Users

7. Click **Add…** to specify the user(s)/group(s) that will have access to the specific devices specified in this protection policy, and click **OK**.



Screenshot 37: Add permissions options - Users

8. Enable or disable Access/Read and Write permissions for each user/group you specified and click **Finish**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers…**.

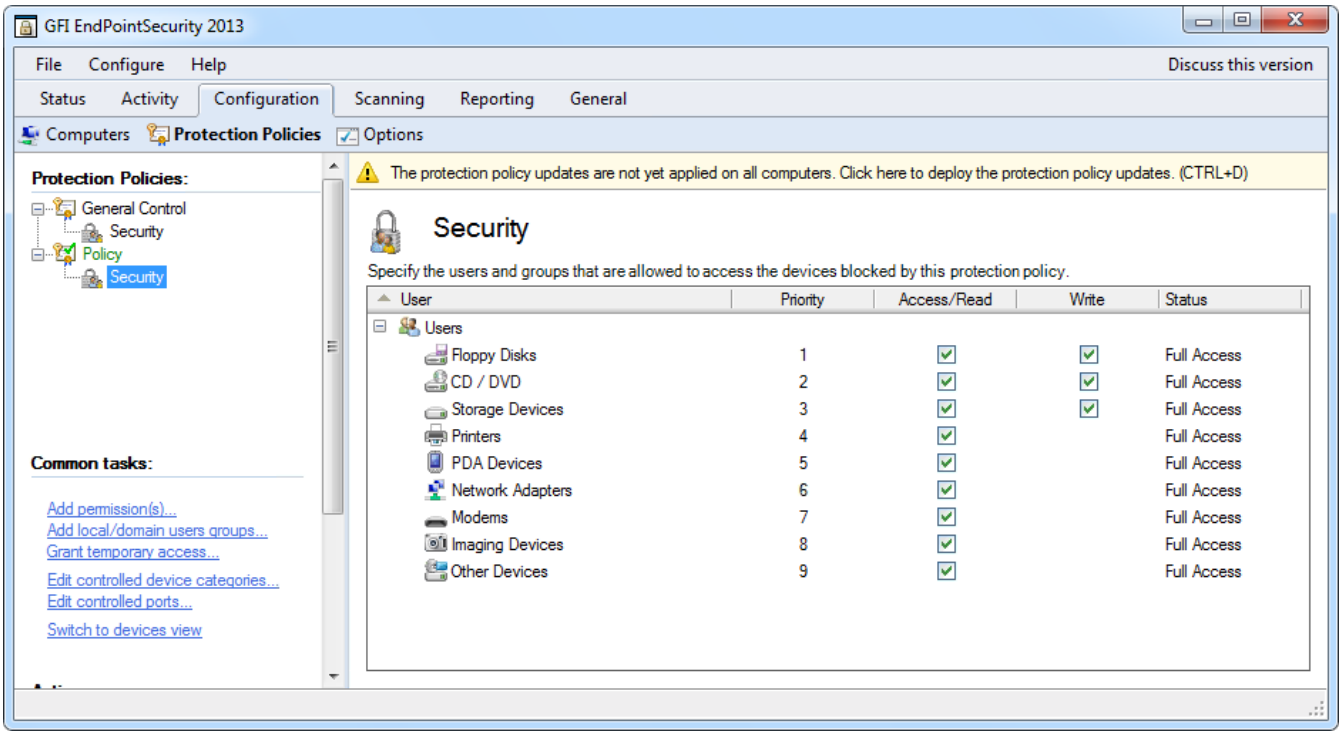
6.7 Viewing access permissions

GFI EndPointSecurity enables you to view all permissions assigned to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis.

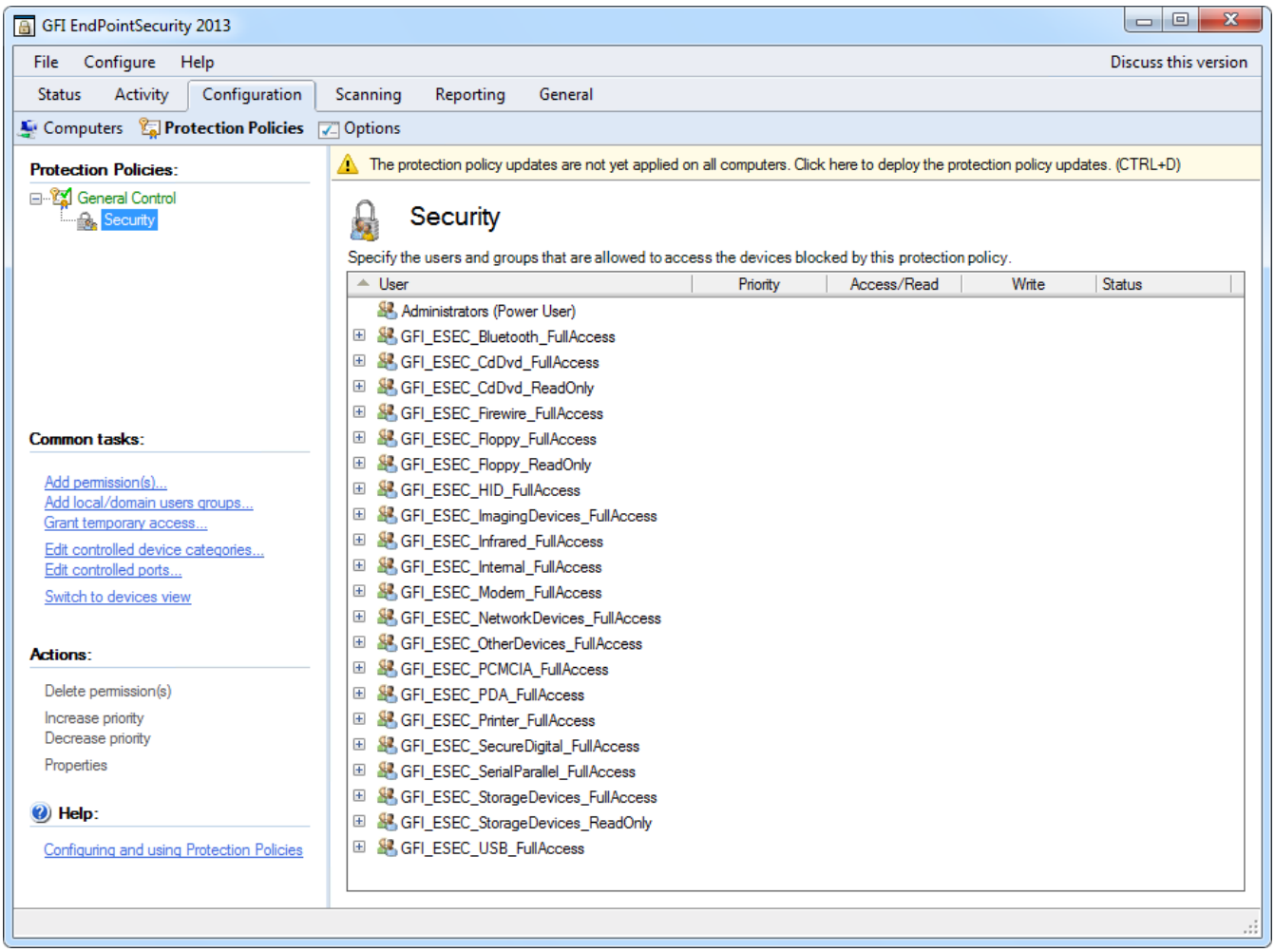
When a device category or connectivity port is not set to be controlled by the particular security policy, the relevant permission is disabled. For more information, refer to Configuring controlled device categories or Configuring controlled connectivity ports.

To view all permissions assigned to users in a protection policy:

1. Click **Configuration** tab **> Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. Click **Security**. In the right pane you can view all the set permissions for this protection policy.



Screenshot 38: Protection Policies sub-tab - devices view



Screenshot 39: Protection Policies sub-tab - users view

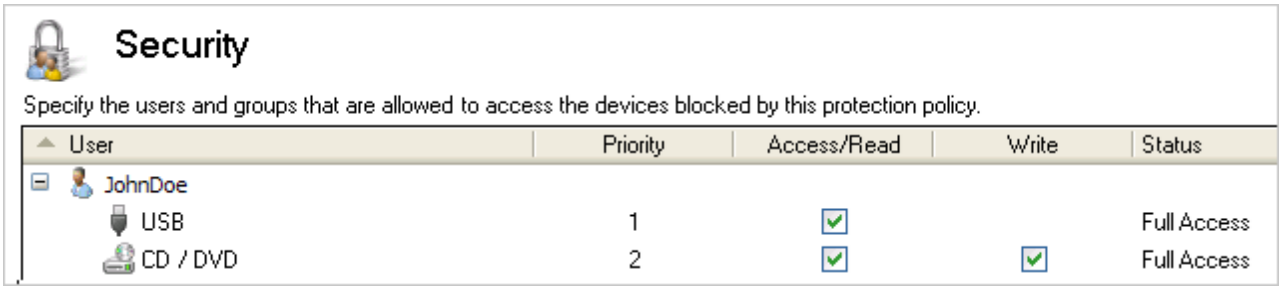
4. From the left pane, click **Switch to devices view** or **Switch to users view** in the **Common tasks** section, to switch grouping of permissions by devices/ports or users.

> **Note**
>
> In users view, you will also see any power users specified within the policy.

6.8 Configuring priorities for permissions

GFI EndPointSecurity enables you to prioritize any permissions assigned to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis and on a user-by-user basis.

For example, for a specific user specified within a specific protection policy, you may decide to give priority 1 to USB port permissions, and priority 2 to CD/DVD drive permissions. This means that if the user connects an external CD/DVD drive via the USB port to the target computer, permissions for the USB port will take precedence over permissions for the CD/DVD drive.



Screenshot 40: Protection Policies sub-tab - Security area

To prioritize permissions assigned to users in a protection policy:

1. Click **Configuration** tab **> Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. Click **Security** sub-node.
4. From the left pane, click **Switch to users view** in the **Common tasks** section, to switch grouping of permissions by users.
5. Right-click the **Security** section and select **Expand all**.
6. Highlight the required device or port.
7. From the left pane, click **Increase priority** or **Decrease priority** in the **Actions** section.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers**….

6.9 Configuring device blacklist

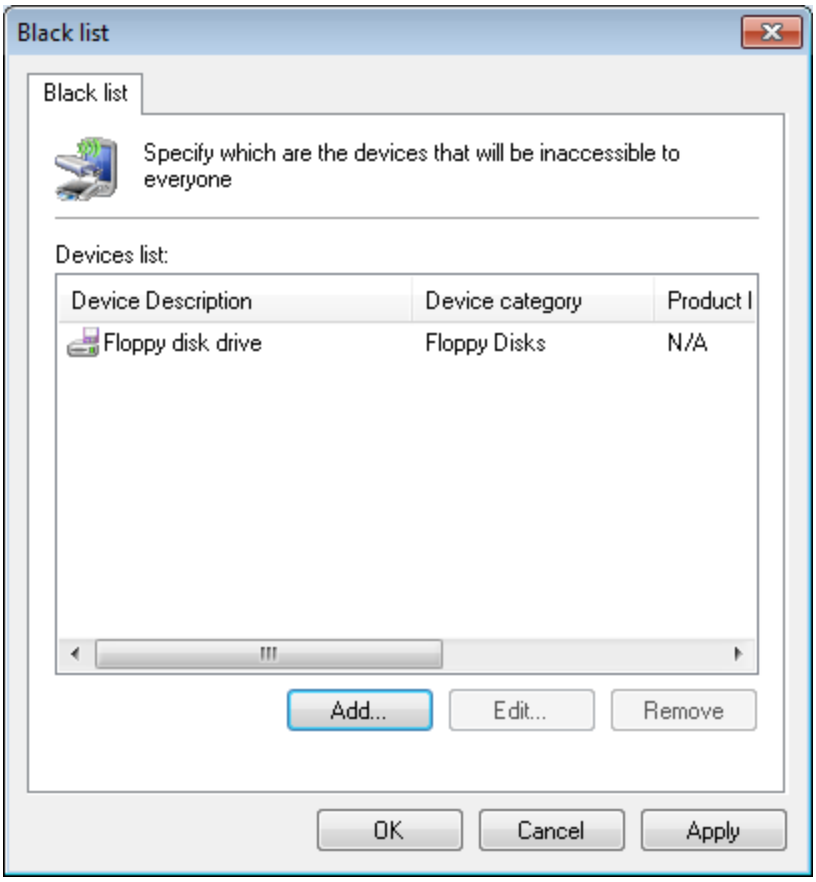
GFI EndPointSecurity enables you to specify which device(s) can be made inaccessible to everyone. The blacklist is granular, so you can even blacklist a specific device with a specific serial number. You can do this on a policy-by-policy basis.

For an updated list of devices currently connected to the target computers, run a device scan and add the discovered devices to the devices database prior to configuring blacklisted devices. For more information, refer to Discovering Devices (page 100).

> **Note**
>
> Power users will override any blacklisted devices, and thus will be able to access blacklisted devices.

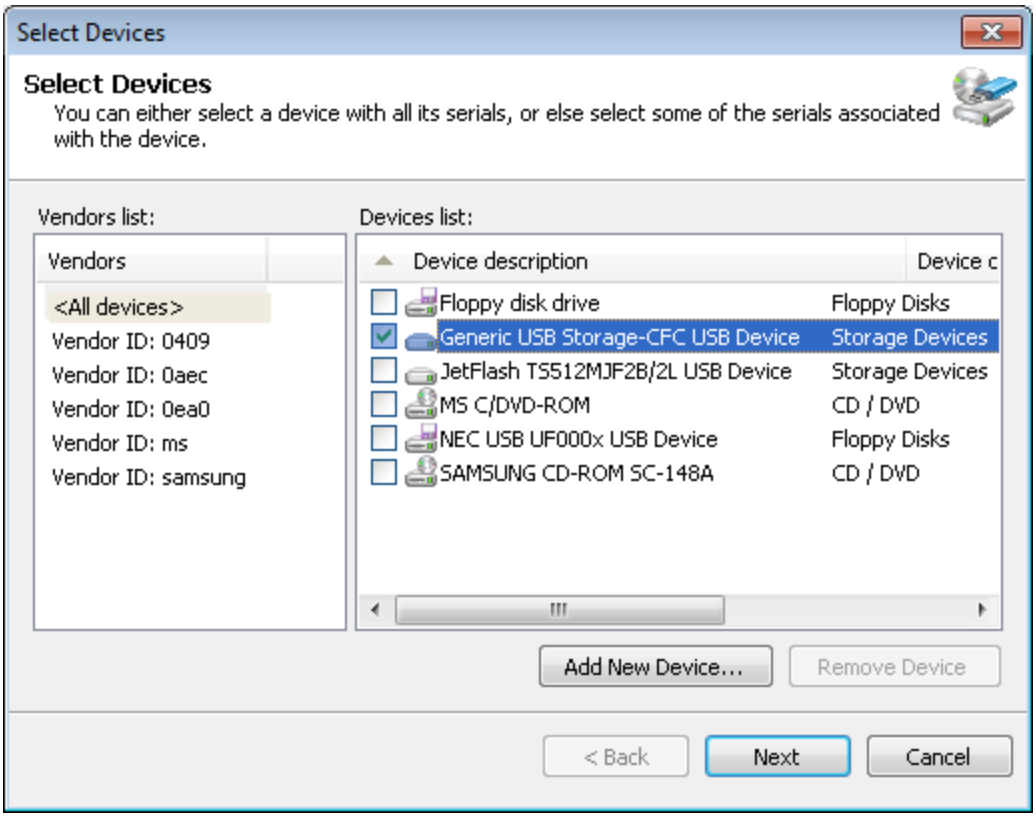
To add devices to the blacklist of a specific protection policy:

1. Click **Configuration** tab > **Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. From the right pane, click **Devices Blacklist** in the **General Control** section.



Screenshot 41: Black list options

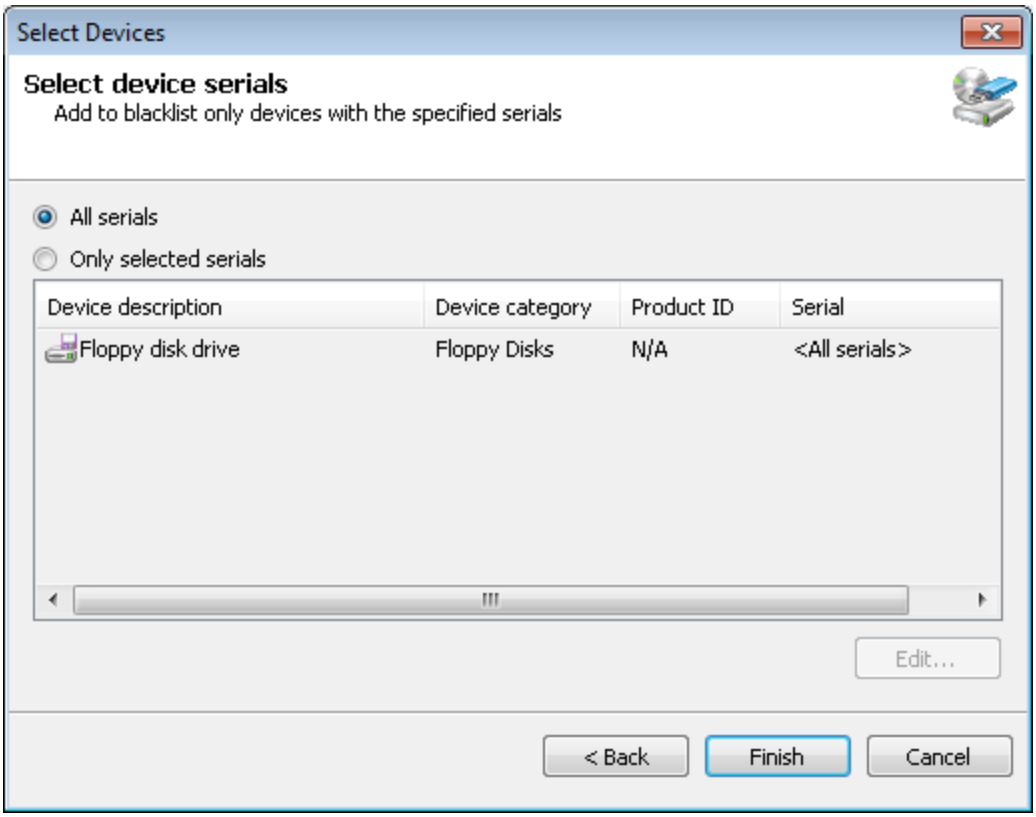
4. In the **Black list** dialog, click **Add…** to select devices to add to the blacklist.



Screenshot 42: Select Devices options

5. In the **Select Devices** dialog enable or disable the devices to add to the blacklist from the Devices list and click **Next**.

> **Note**
>
> If a required device is not listed, click **Add New Device…** to specify the details of the device you want to add to the blacklist, and click **OK**.

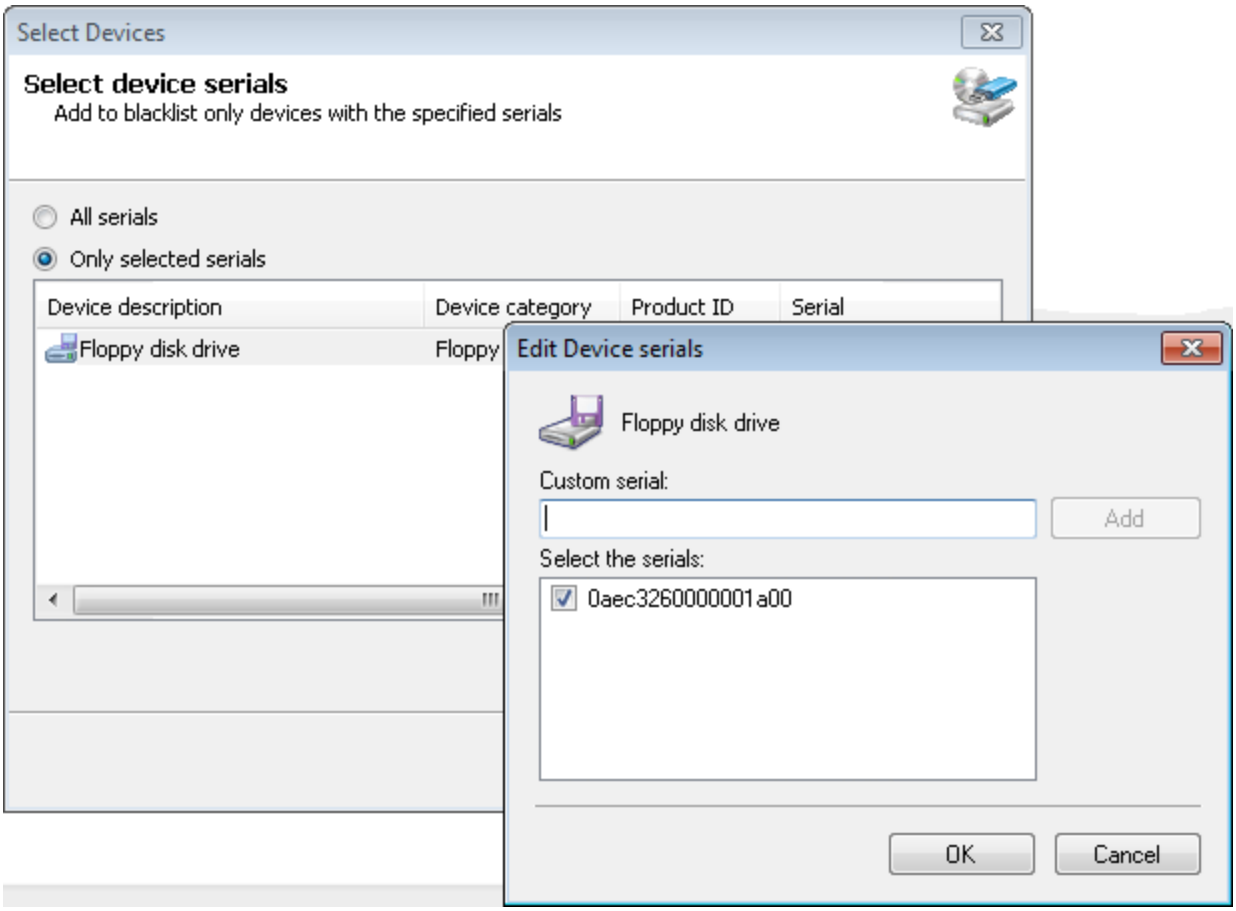


Screenshot 43: Select Devices options - Select device serials

6. Select the required serials related option from:

» **All serials** - to blacklist all serial numbers of a specific device. Click **Finish** and **OK**.

» **Only selected serials** - to specify particular device serial number(s) to be added to the blacklist. Next, highlight the device and click **Edit...** to specify the serial number(s). Click **OK**, **Finish** and **OK**.



Screenshot 44: Select Devices options - Edit Device serials

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers**….

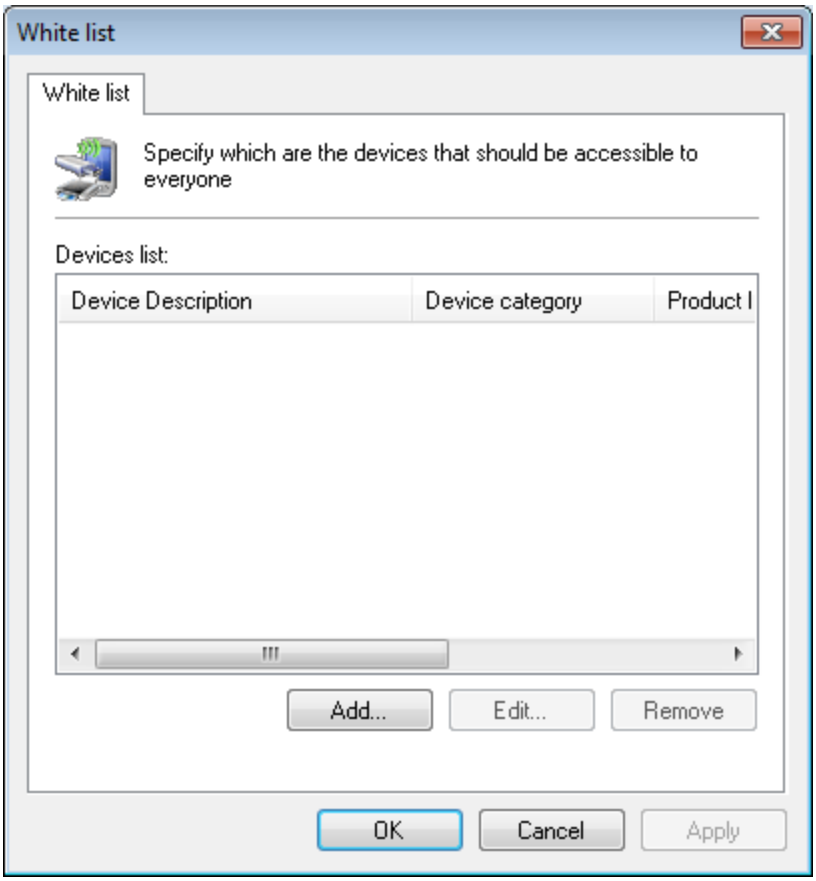
6.10 Configuring device whitelist

GFI EndPointSecurity enables you to specify which device(s) can be accessed by everyone. The whitelist is granular, so you can even whitelist a specific device with a specific serial number. You can do this on a policy-by-policy basis.

For an updated list of devices currently connected to the target computers, run a device scan and add the discovered devices to the devices database prior to configuring whitelisted devices. For more information, refer to Discovering Devices (page 100).

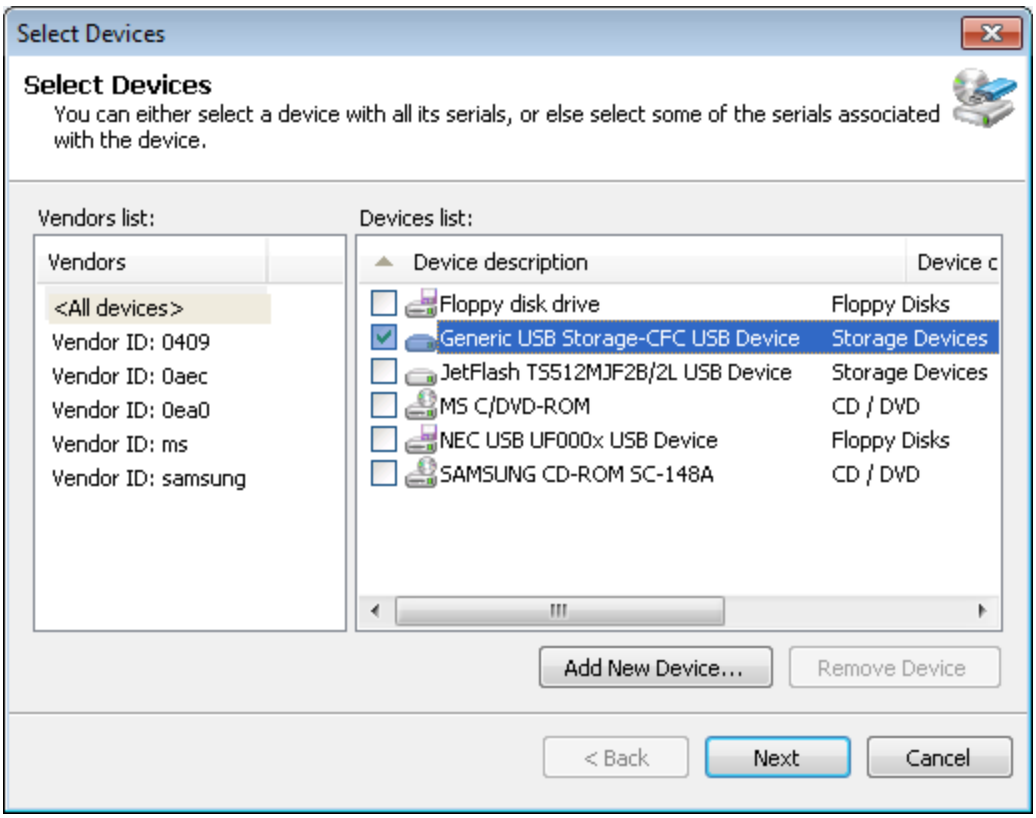
To add whitelist devices to a protection policy:

1. Click **Configuration** tab **> Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. From the right pane, click **Devices WhiteList** in the **General Control** section.



Screenshot 45: White list options

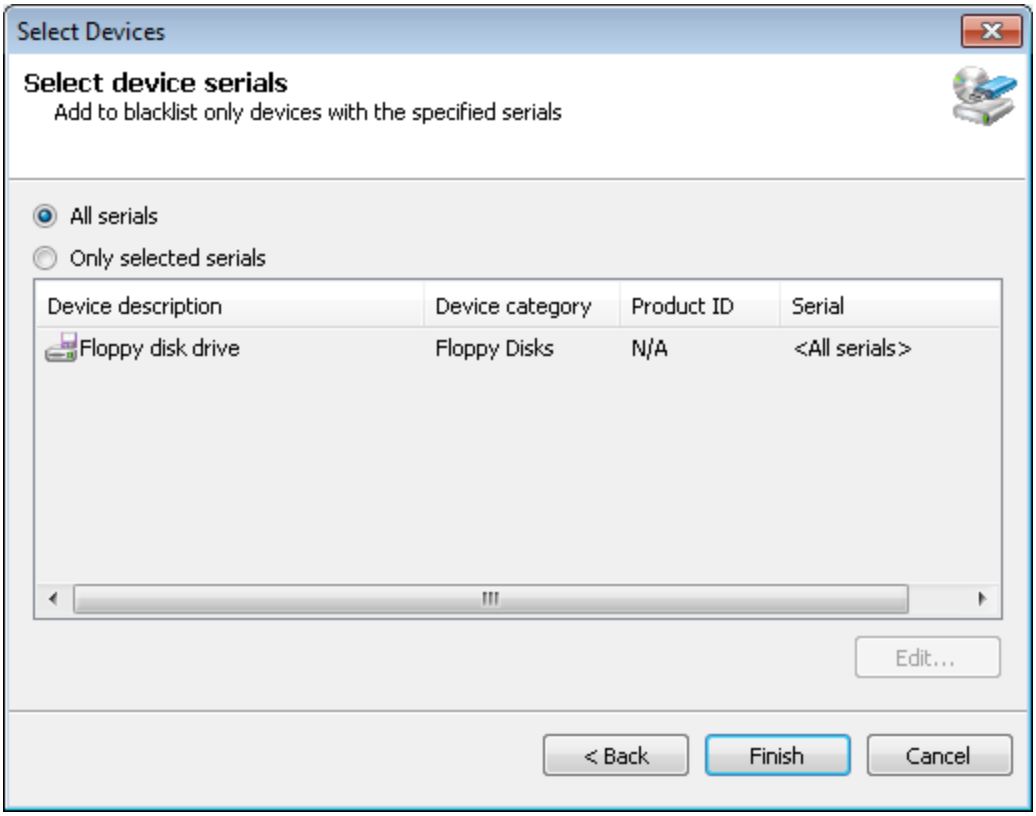
4. In the **Whitelist** dialog, click **Add…** to select devices to add to the whitelist.



Screenshot 46: Select Devices options

5. In the **Select Devices** dialog enable or disable the devices to add to the whitelist from the Devices list, and click **Next**.

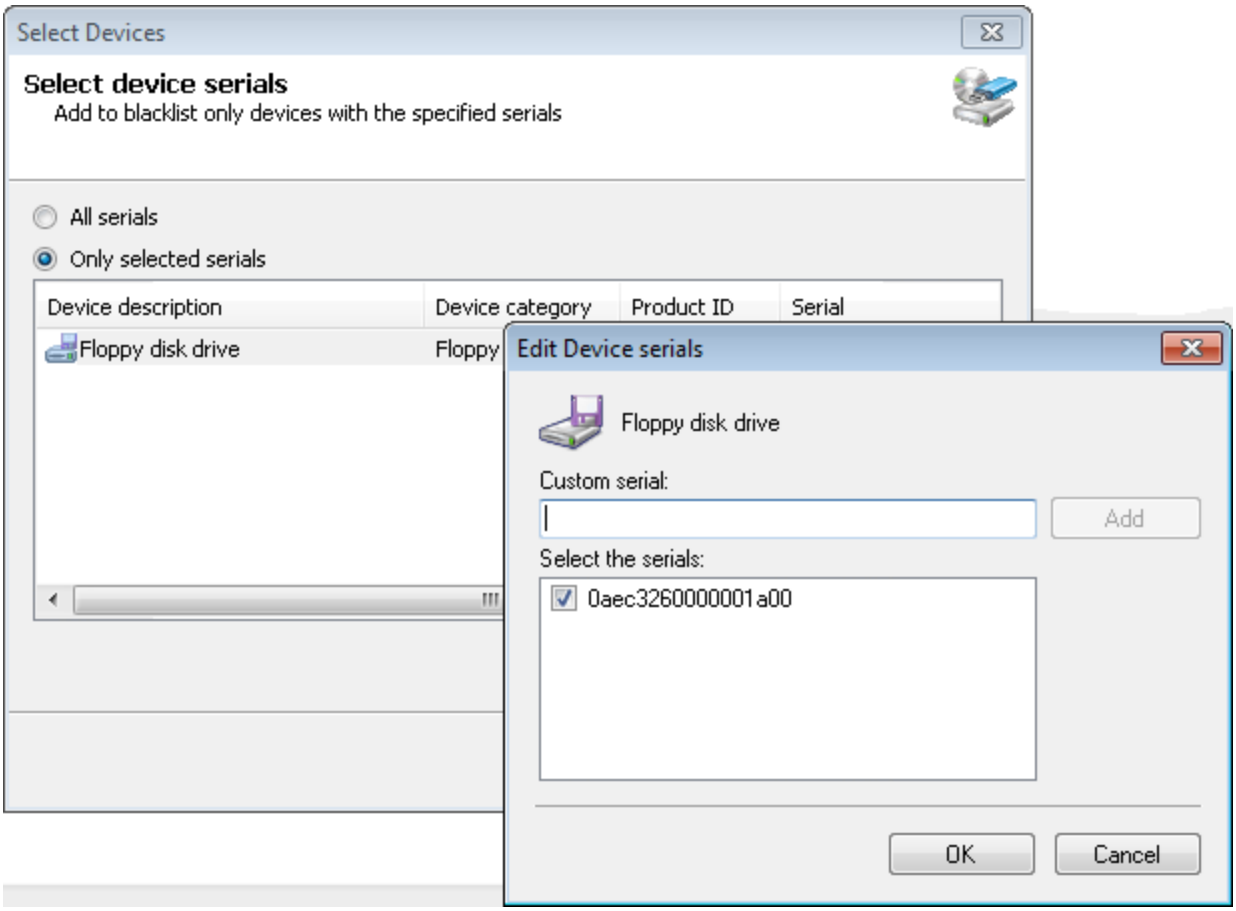
> **Note**
>
> If a required device is not listed, click **Add New Device…** to specify the details of the device you want to add to the whitelist, and click **OK**.



Screenshot 47: Select Devices options - Select device serials

6. Select the required serials related option from:

- **All serials** - to whitelist all serial numbers of a specific device. Click **Finish** and **OK**.
- **Only selected serials** - to specify that only particular device serial number(s) are to be added to the whitelist. Next, highlight the device and click **Edit…** to select the serial number(s) to white-list. Click **OK**, **Finish** and **OK**.



Screenshot 48: Select Devices options - Edit Device serials

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers**….

6.11 Configuring temporary access privileges

GFI EndPointSecurity enables you to grant temporary access to users. This enables them to access devices and connection ports on protected target computers for a specified duration/time window. You can do this on a policy-by-policy basis.

When temporary access is granted, any permissions and settings (e.g. file-type filters) set in the protection policy applicable for the target computer, are temporarily overridden.

For more information, refer to How GFI EndPointSecurityworks - Temporary Access (page 17).

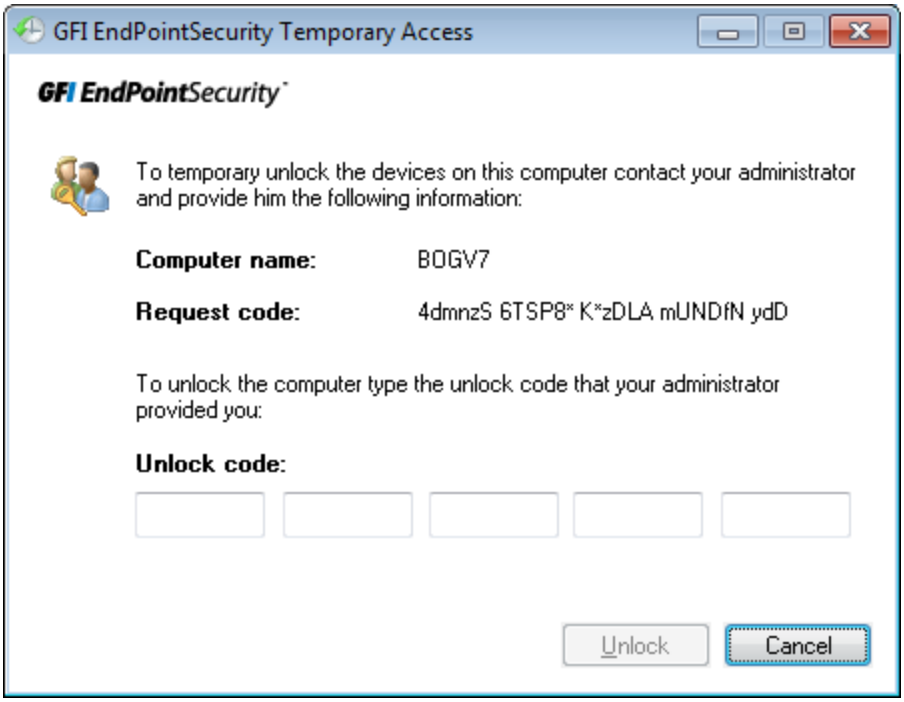
- Requesting temporary access for a protected computer
- Granting temporary access to a protected computer.

6.11.1 Requesting temporary access for a protected computer

To generate a request code: tool:

Screenshot 49: Devices Temporary Access icon

1. From the **Control Panel** click **Devices Temporary Access**.



Screenshot 50: GFI EndPointSecurityTemporary Access tool

2. In the **GFI EndPointSecurity Temporary Access** dialog take note of the **Request code** generated. Communicate the following details to your security administrator:

- Request code
- Device/connection port type
- When you require access
- For how long you require access.

Keep the GFI EndPointSecurity Temporary Access tool open.

3. When the administrator sends the unlock code, key it in the **Unlock code** field.

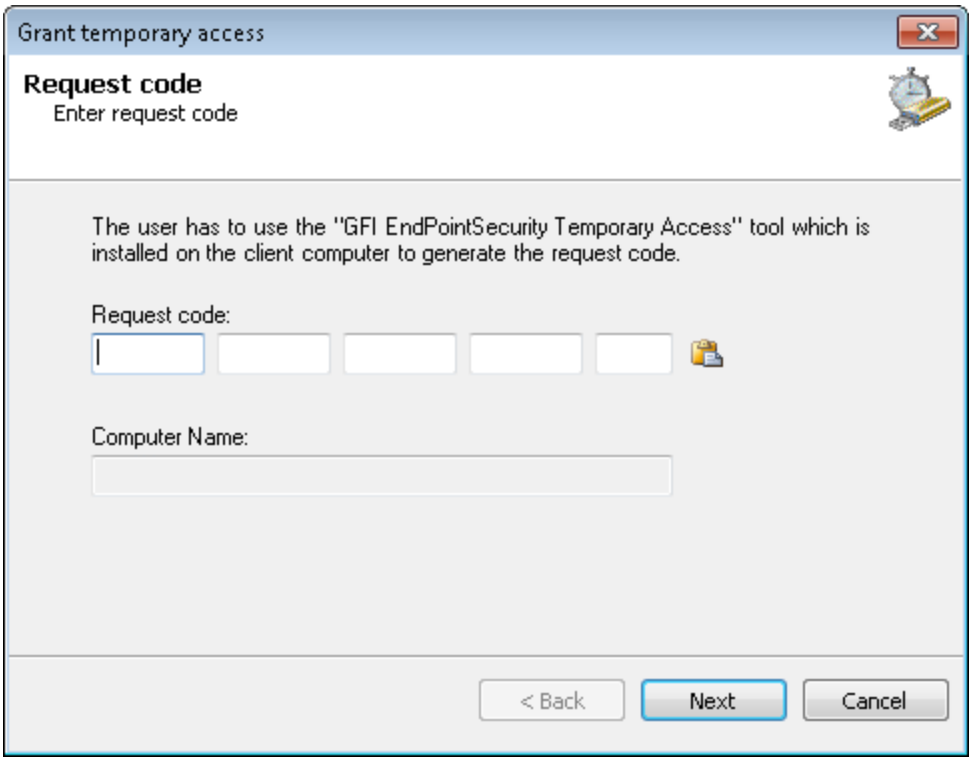
> **Note**
>
> An unlock code keyed in on the protected target computer outside the specified validity period will not activate temporary access.

4. Click **Unlock** to activate temporary access. You are now able to access the required device and/or connection port.

6.11.2 Granting temporary access to a protected computer

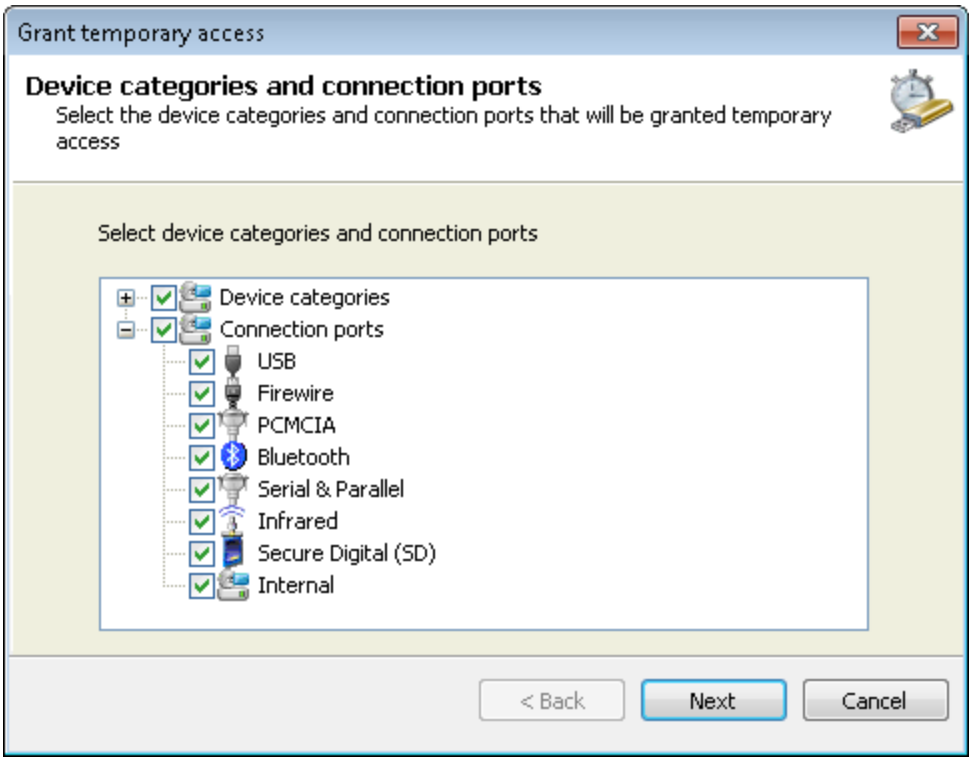
To grant temporary access:

1. From GFI EndPointSecurity management console, click **Configuration** tab > **Protection Policies** sub-tab.
2. From the left pane, select the protection policy that includes the computer on which temporary access needs to be granted.
3. From the right pane, click **Grant temporary access** in the **Temporary Access** section.



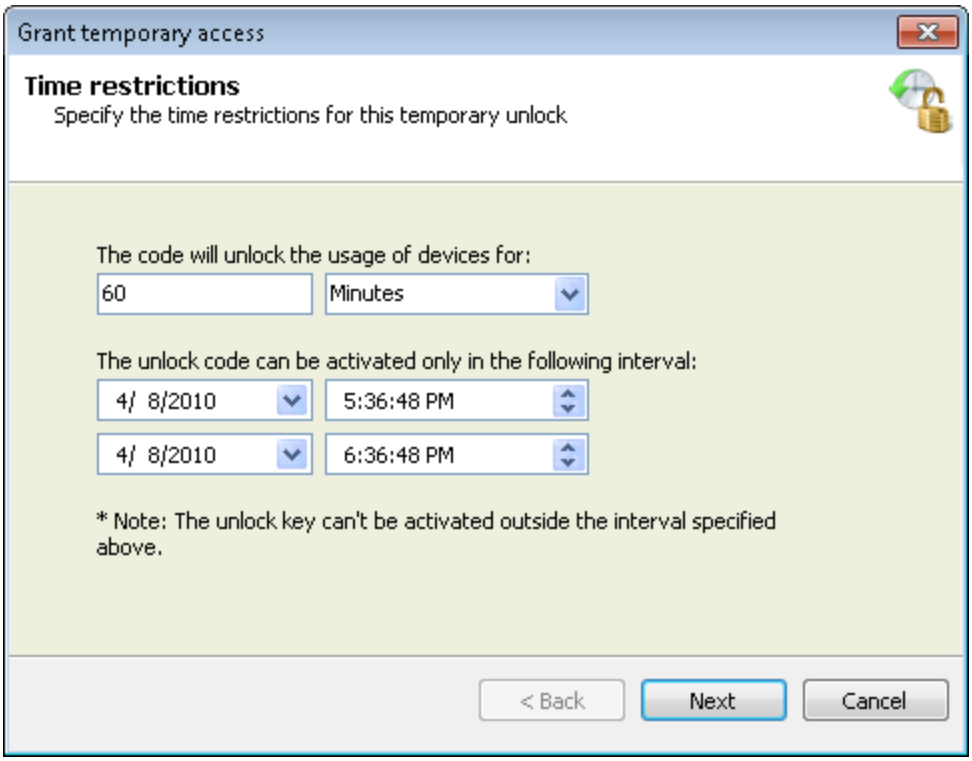
Screenshot 51: Grant temporary access options - Request code

4. In the **Grant temporary access** dialog key in the request code received from the user, in the **Request code** field. The computer name from which the request code was generated, is displayed in the **Computer Name** field. Click **Next**.



Screenshot 52: Grant temporary access options - Device categories and connection ports

5. Enable the required device categories and/or connection ports from the list, to which you will be granting temporary access, and click **Next**.



Screenshot 53: Grant temporary access options - Time restrictions

6. Specify the duration during which access is allowed, and the validity period of the unlock code, and click **Next**.

7. Take note of the **Unlock code** generated. Communicate the code to the user requesting temporary access and click **Finish**.

6.12 Configuring file-type filters

GFI EndPointSecurity enables you to specify file-type restrictions on files, such as .DOC or .XLS files, being copied to/from allowed devices. You can apply these restrictions to Active Directory (AD) users and/or user groups. You can do this on a policy-by-policy basis.

Filtering is based on file extension checks and real file type signature checks. Real file type signature checking can be done on the following file types:

AVI	BMP	CAB	CHM	DLL	DOC	EMF	EXE	GIF	HLP
HTM	JPE	JPEG	JPG	LNK	M4A	MDB	MP3	MPEG	MPG
MSG	MSI	OCX	P7M	PDF	PPT	RAR	RTF	SCR	SYS
TIF	TIFF	TXT	URL	WAV	XLS	ZIP	DOCX	XLSX	PPTX

Note 1

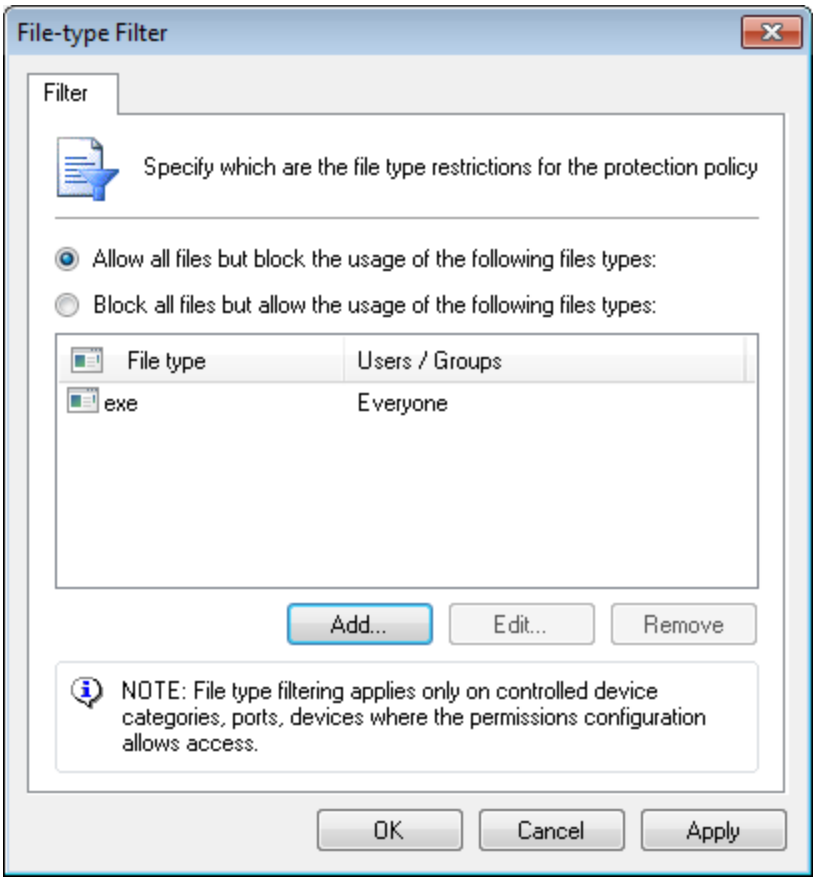
For any other file type not specified above, filtering is based only on the file extension.

Note 2

File-type filtering is only applied to device categories and/or ports for which permissions have been set to allow access.

To configure file-type restrictions for users in a specific protection policy:

1. From GFI EndPointSecurity management console, click **Configuration** tab > **Protection Policies**.
2. From the left pane, select the protection policy for which you want to specify file-type restrictions.
3. From the right pane, click **File-type Filter** in the **File control** section.

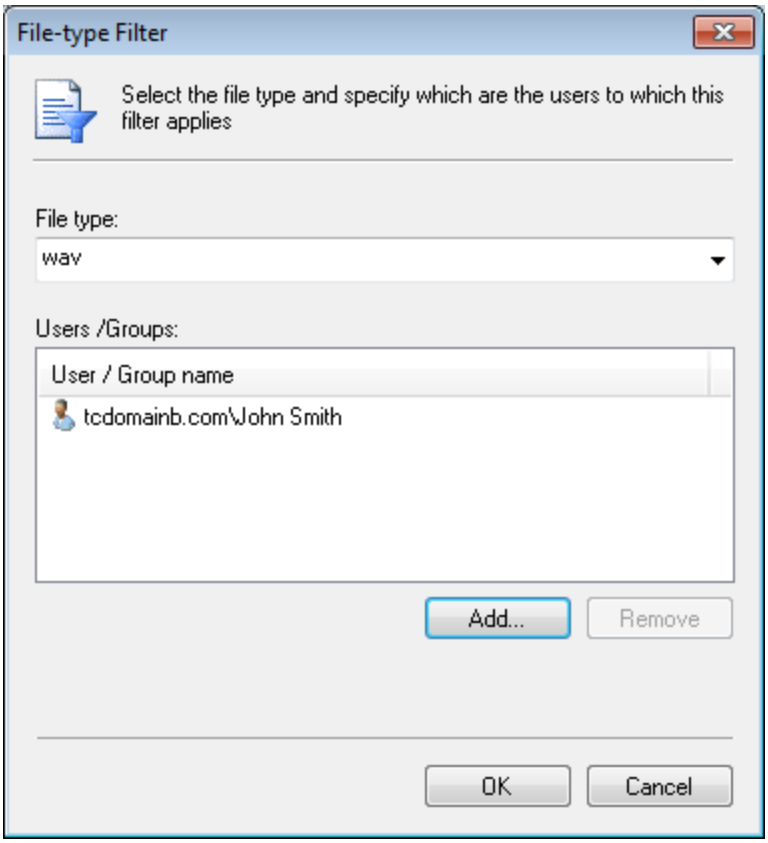


Screenshot 54: File-type Filter options

4. In the File-type Filter dialog select the restriction to apply to this policy:

» Allow all files but block the usage of the following file types

» Block all files but allow the usage of the following file types.



Screenshot 55: File-type Filter and user options

5. Click **Add…** and select or key in the file-type from the **File type** drop-down list.
6. Click **Add…** to specify the user(s)/group(s) who are allowed/blocked from accessing the specified file-type, and click **OK**. Repeat the preceding two sub-steps for each file type to restrict.
7. Click **OK** twice.

To deploy protection policy updates on target computers specified in the policy:

1. From GFI EndPointSecurity management console, click **Configuration** tab **> Computers** sub-tab.
2. From the left pane, click **Deploy to all computers…** in the **Common tasks** section.

6.13 Configuring content awareness

GFI EndPointSecurity enables you to specify the file content restrictions for a particular protection policy. The content awareness feature looks into files transiting the endpoints via removable devices and it \identifies content based on pre-configured and custom regular expressions and dictionary files. By default the module looks for secure confidential details such as social security numbers and primary account numbers as well as information related to companies and enterprises such as names of diseases, drugs, dangerous chemicals and also trivial language or ethnic / racist terms.

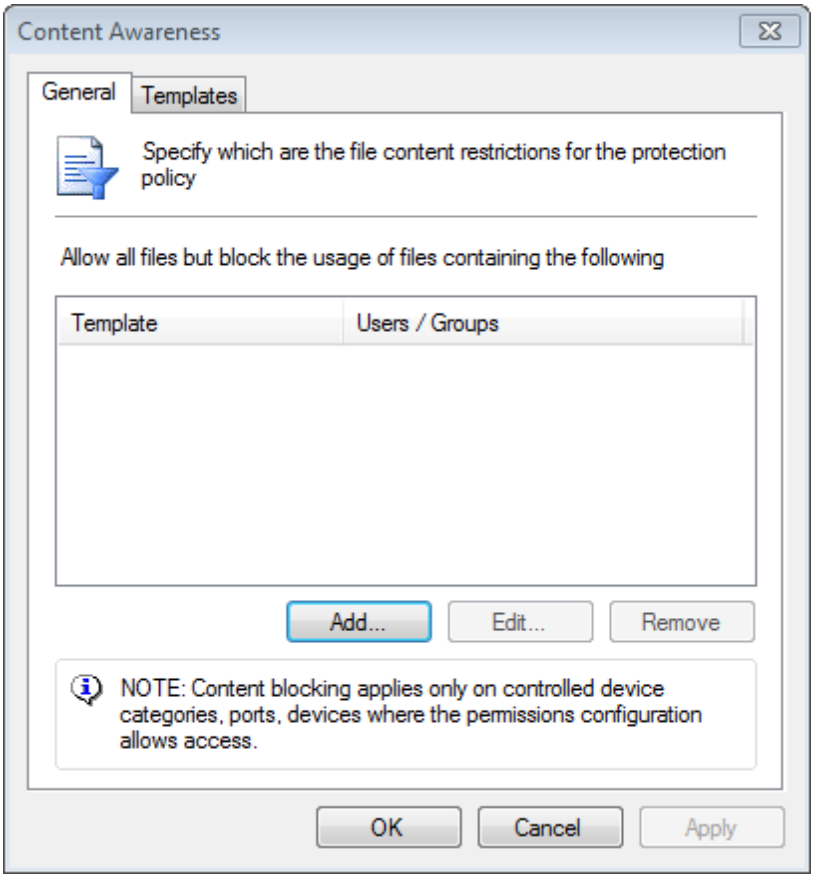
» You can configure content checking as a global policy in a similar fashion to the file checking module.

6.13.1 Managing content awareness options

To configure content awareness options for users

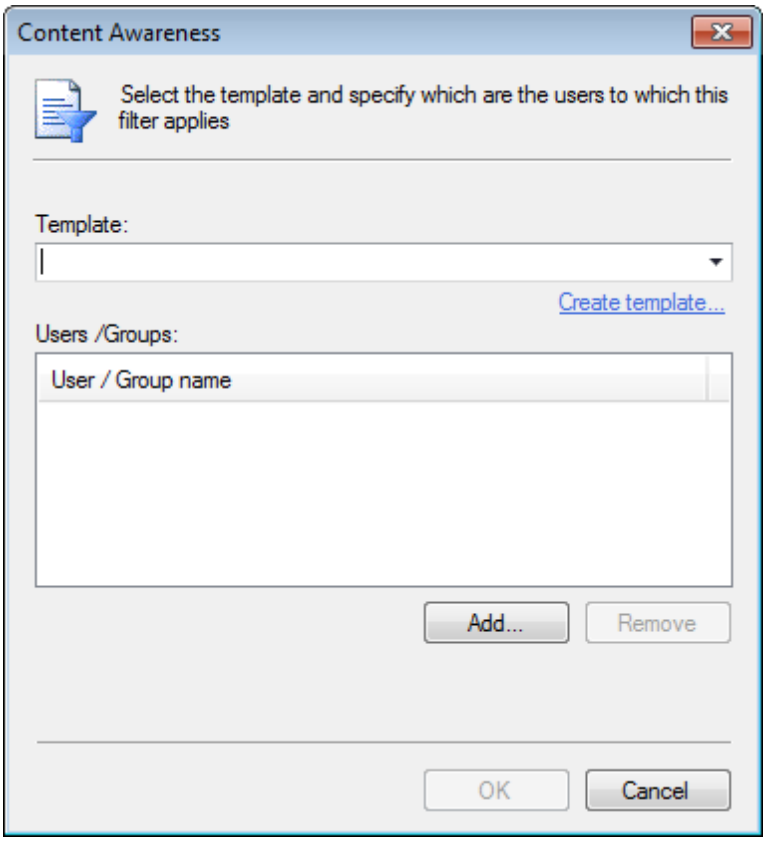
in a specific protection policy:

1. From GFI EndPointSecurity management console, click **Configuration** tab **> Protection Policies**.
2. From the left pane, select the protection policy for which to specify content restrictions.
3. From the right pane, click **Content awareness** in the **File control** section.



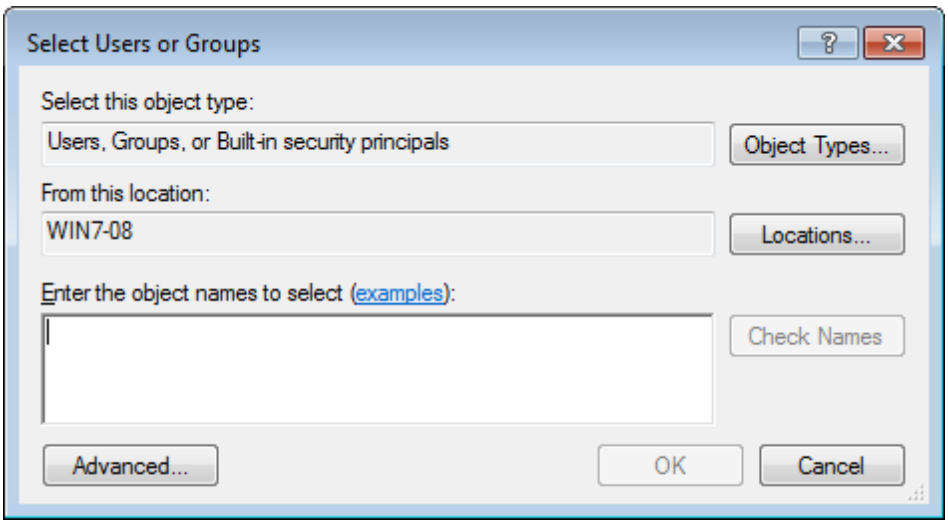
Screenshot 56: Content awareness options

4. In the Content awareness dialog, click **Add** to select the template to apply to this policy:



Screenshot 57: Add a new template

5. Click **Add…** and select or key in the template from the **Template** drop-down list.
6. Click **Add…** to specify the user(s)/group(s) and click **OK**. Repeat the preceding two sub-steps for each template that will be applied.
7. Click **OK**.

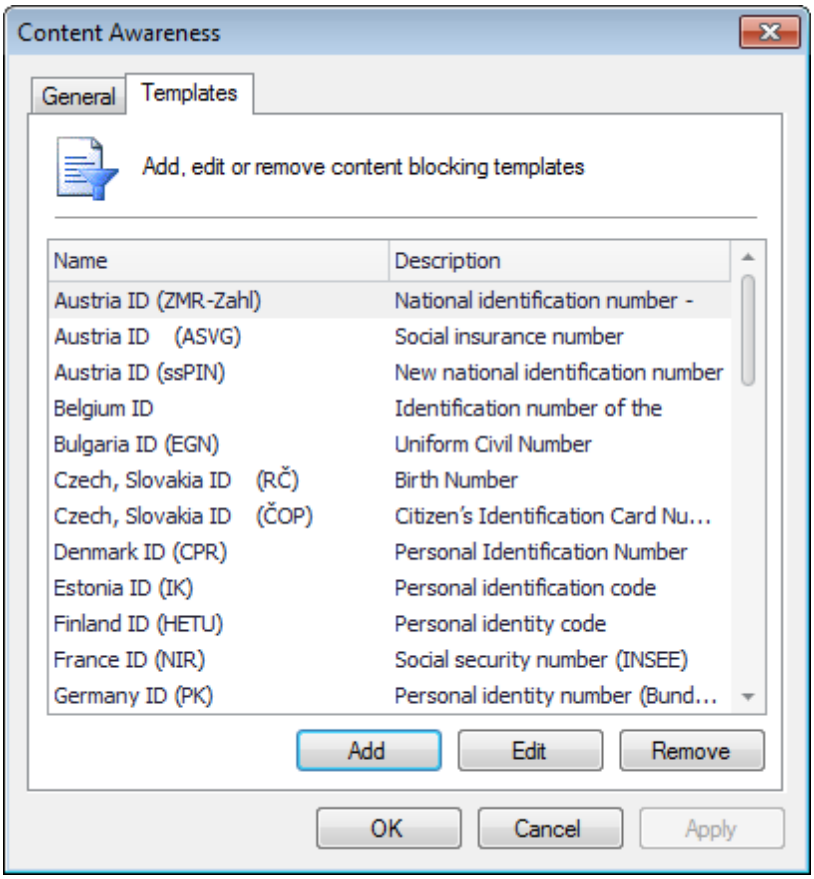


Screenshot 58: Selecting users or groups

6.13.2 Managing template options

To add, edit or remove predefined templates:

1. Click **Templates** and select a template from the **Template** list.
2. Click **Add**, **Edit** or **Remove** to change or delete templates.

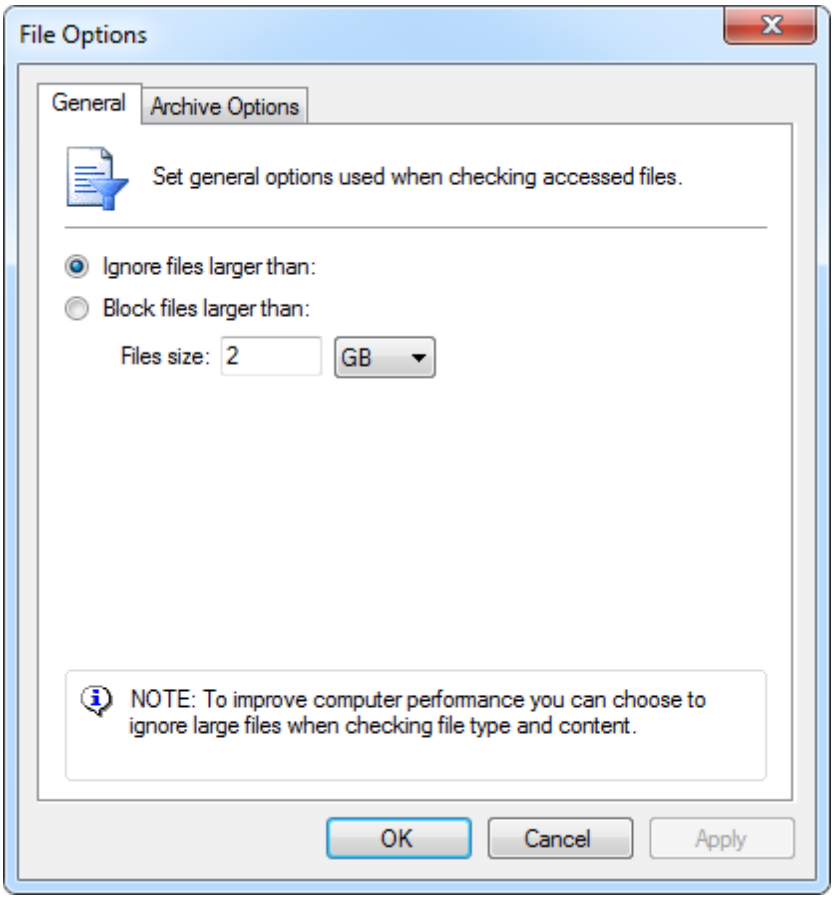


Screenshot 59: Managing templates

6.14 Configuring file options

GFI EndPointSecurity enables you to specify the options required to block or allow files based on size. GFI EndPointSecurity also enables you to ignore large files when checking file type and content and archived files.

1. From GFI EndPointSecurity management console, click **Configuration** tab > **Protection Policies**.
2. From the left pane, select the protection policy for which you want to specify file options restrictions.
3. From the right pane, click **File options** in the **File control** section.

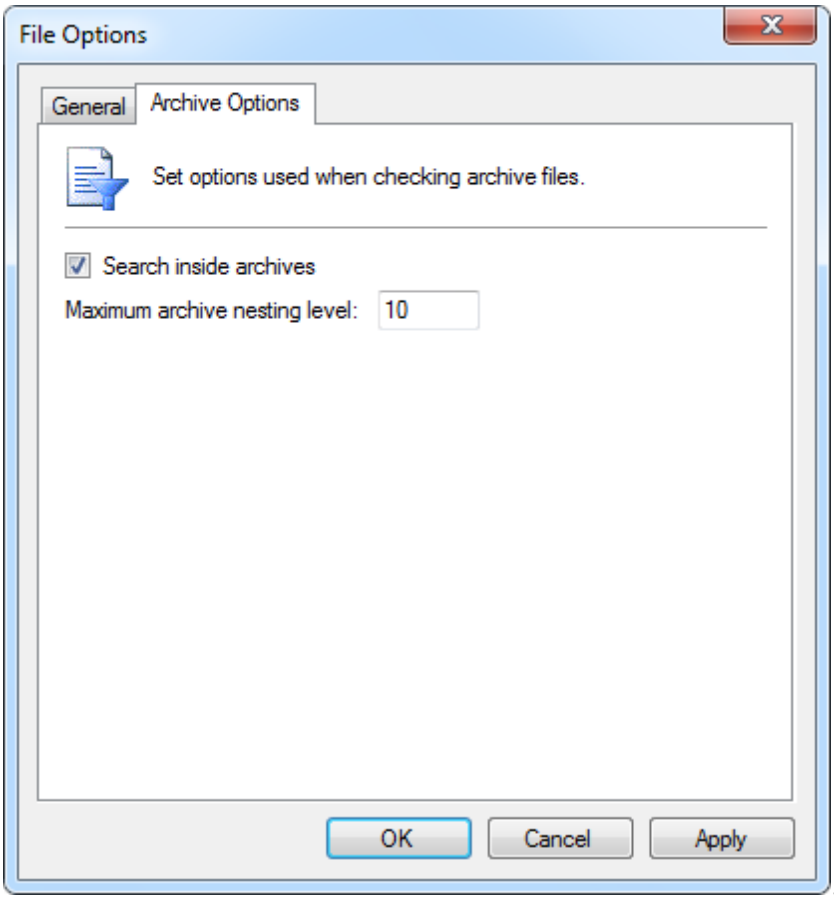


Screenshot 60: File options

4. In the File options dialog select from the following options:

Table 13: File options - User options

Option	Description
Ignore files larger than:	Ignores files larger than the specified size when checking accessed files
Block files larger than :	Blocks files larger than the specified size when checking accessed files



Screenshot 61: File-type Filter and user options

5. From the **Archive Options** tab, enable / disable **Search inside archives** and specify the archive nesting level to use when checking archive files.
6. Click **OK**.

6.15 Configuring security encryption

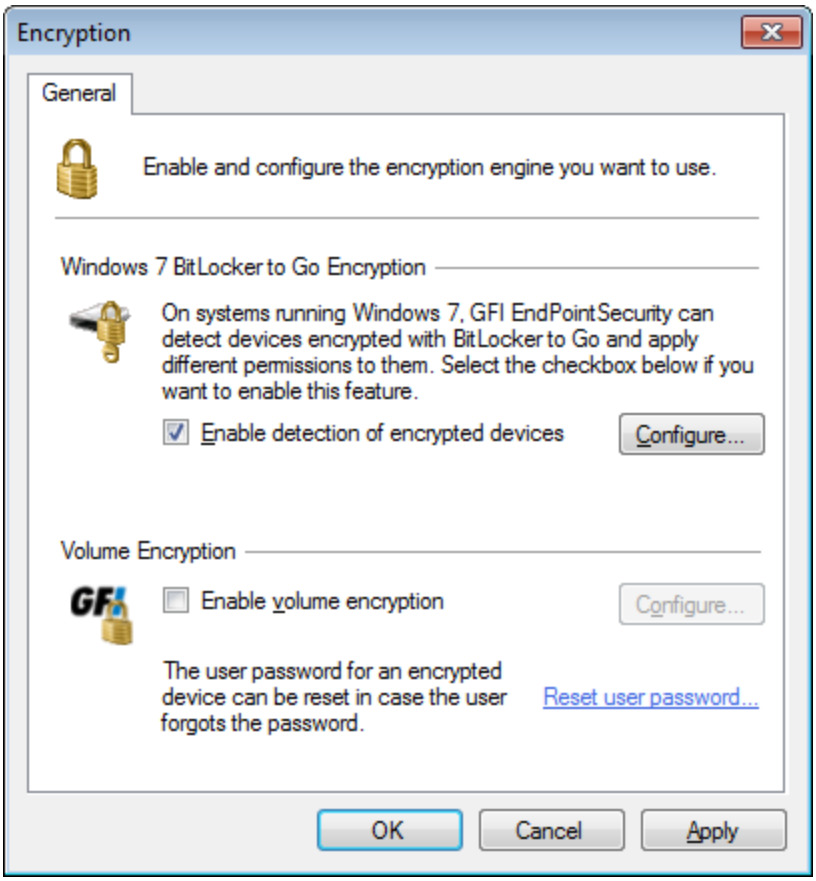
GFI EndPointSecurity enables you to configure settings which specifically cater for encrypted devices. It also enables you to encrypt devices which are not yet secured.

- Configuring Microsoft BitLocker To Go devices
- Configuring Volume Encryption

6.15.1 Configuring Microsoft BitLocker To Go devices

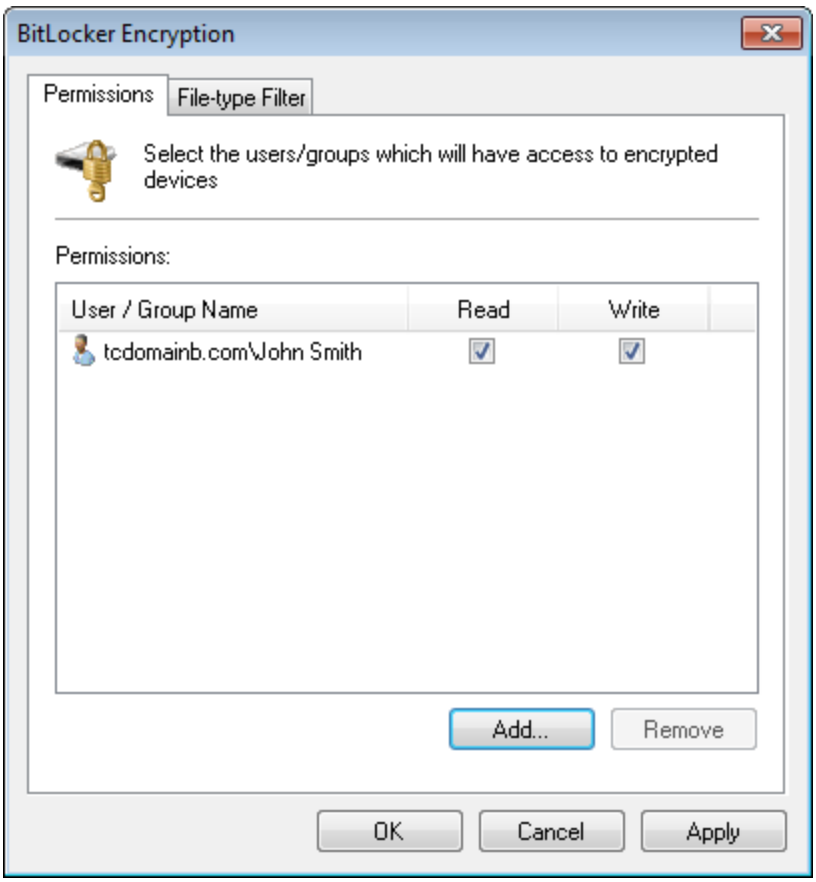
GFI EndPointSecurity can detect storage devices encrypted with Microsoft BitLocker To Go. This enables you to configure different permissions on such devices. To enable Microsoft BitLocker To Go detection:

1. From GFI EndPointSecurity management console, click **Configuration** tab > **Protection Policies**.
2. From the left pane, select the protection policy for which to apply the encryption policy.
3. From the right pane, click **Encryption** in the **Security** section.



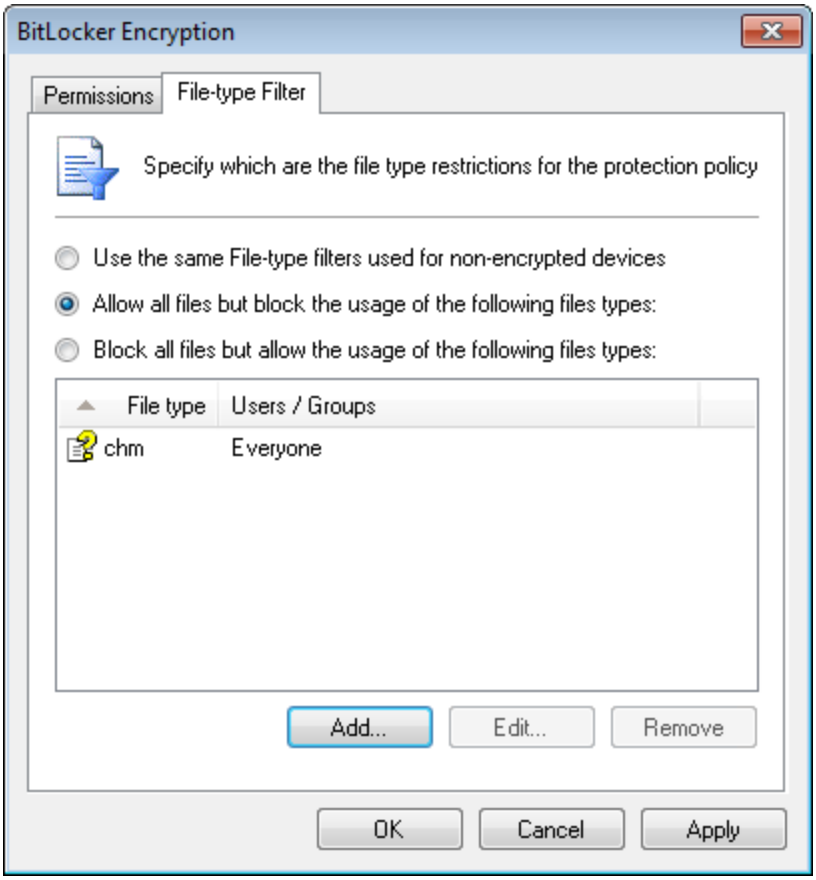
Screenshot 62: Encryption options - General tab

4. Select **Enable detection of encrypted devices** and click **Configure**.



Screenshot 63: Encryption options - Permissions tab

5. Click **Add…** to specify the users and groups with access to encrypted devices.



Screenshot 64: Encryption options - File-type Filter tab

6. Select the **File-type Filter** tab to configure the file-types to restrict.
7. Select the restriction to apply to this policy:

» Use the same File-type filters used for non-encrypted devices

» Allow all files but block the usage of the following file types

» Block all files but allow the usage of the following file types.

8. Use the **Add**, **Edit** and **Remove** buttons, to manage file types.
9. Click **OK**.

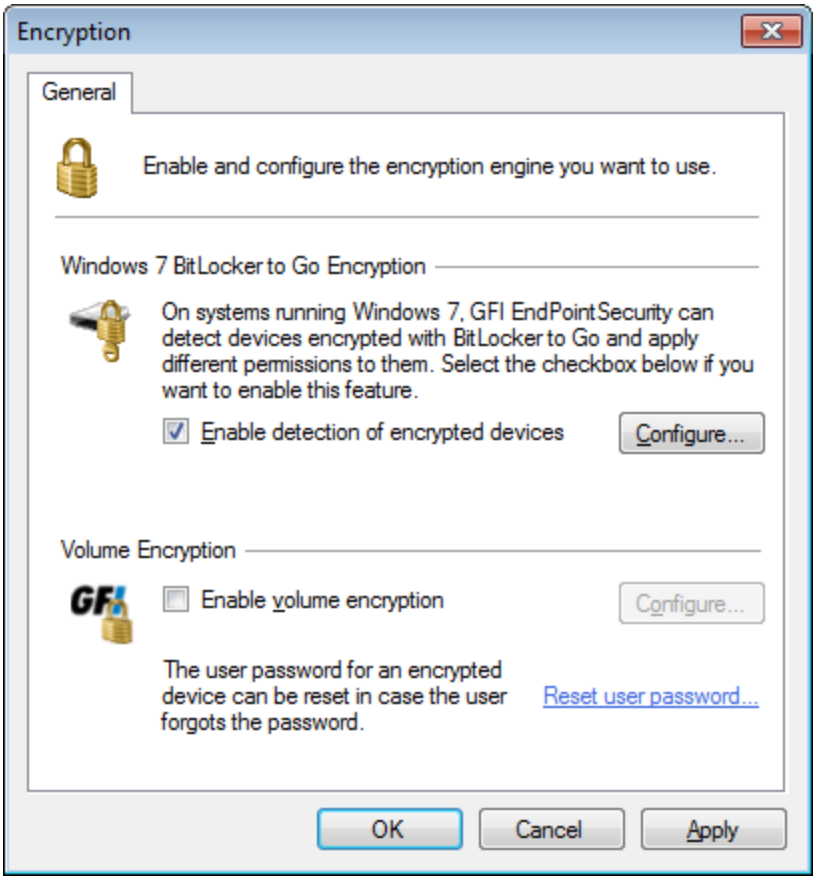
6.15.2 Configuring Volume Encryption

Volume Encryption enables you to encrypt the contents of USB devices using AES 256 encryption. When volume encryption is enforced, users must provide a password to encrypt or access storage devices data. To enforce Volume Encryption on installed agents:

Note

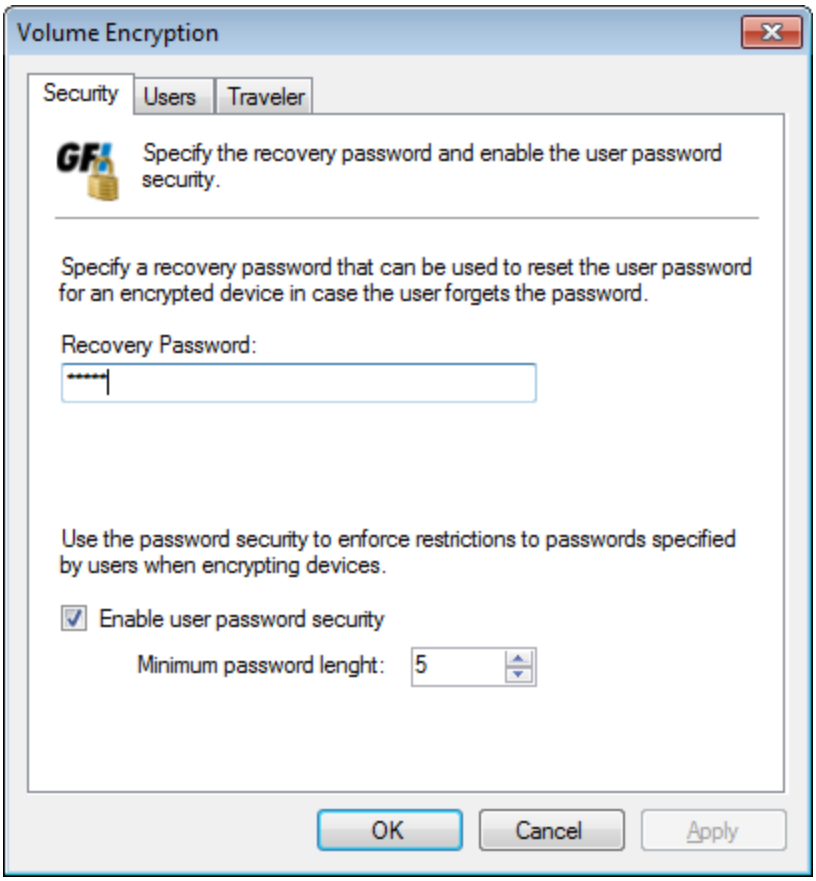
Encryption on demand is possible even if not forced by the administrator directly by the end user by clicking the **Encrypt...** entry from the shell context menu of a removable drive.

1. From GFI EndPointSecurity management console, click **Configuration** tab **> Protection Policies**.
2. From the left pane, select the protection policy for which to apply encryption policy.
3. From the right pane, click **Encryption** in the **Security** section.



Screenshot 65: Encryption options - General tab

4. Select **Enable volume encryption**. Click **Configure**. Click **Reset user password** to reset the encryption password for a specific user.

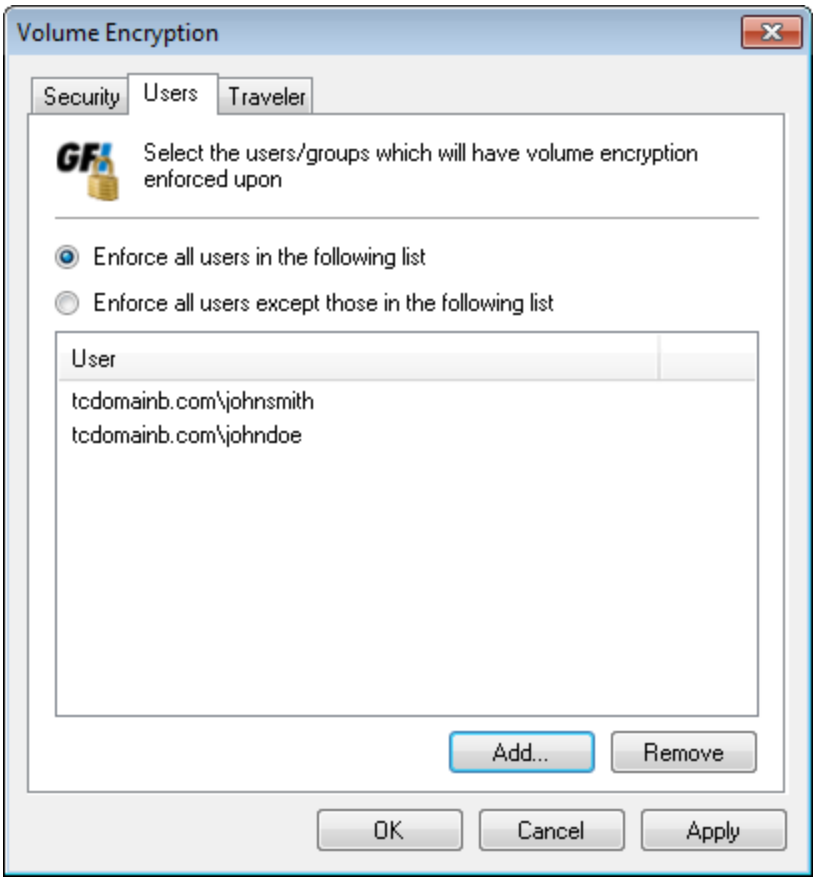


Screenshot 66: Encryption options -Security tab

5. From the **Security** tab, configure the features described below:

Table 14: Volume encryption - Security options

Option	Description
Recovery Password	Key in a password used if users forget or lose their passwords.
Enable user password security	Enforce restrictions to passwords specified by end users. In **Minimum password length**, specify the minimum acceptable password length.

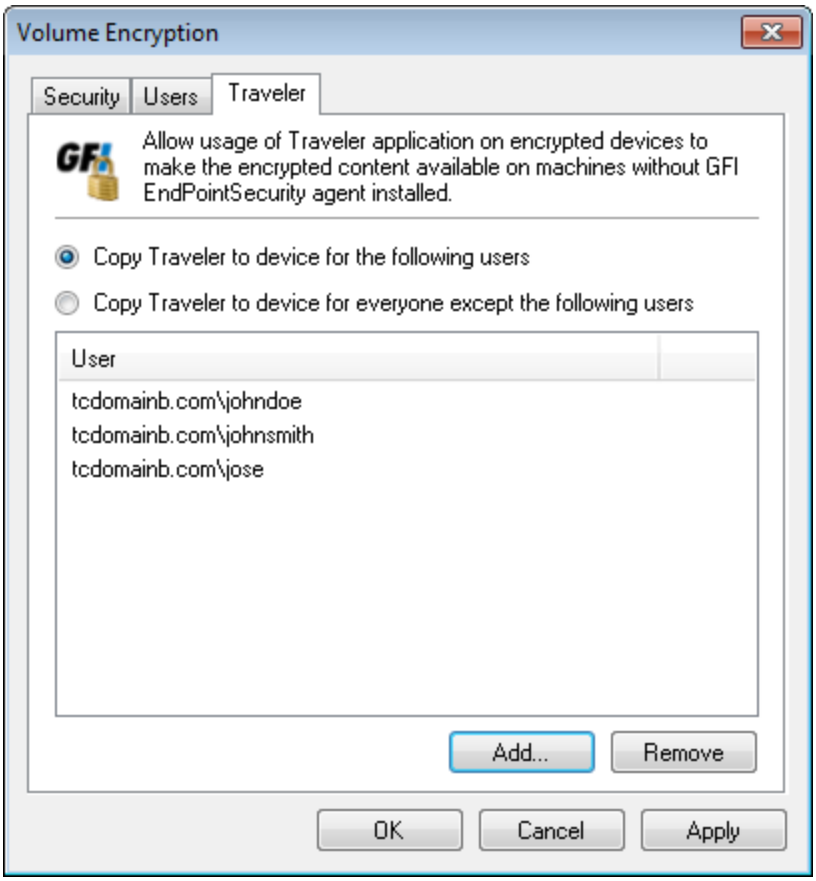


Screenshot 67: Encryption options - Users tab

6. Select **Users** tab and configure the following options:

Table 15: Volume encryption - User options

Option	Description
Enforce all users in the following list	Select the users that will have volume encryption enforced on their portable devices. Use the **Add** and **Remove** buttons to manage selected users.
Enforce all users except those in the following list	Select the users that will be exempt from volume encryption. Use the Add and Remove buttons to manage selected users.



Screenshot 68: Encryption options - Traveler tab

Note

Traveler is an application that can be automatically installed on storage devices using GFI EndPointSecurity. This application enables you to un-encrypt data encrypted by GFI EndPointSecurity on storage devices, from computers that are not running a GFI EndPointSecurity Agent.

7. Select **Traveler** tab and configure the following options:

Table 16: Volume encryption - Traveler options

Option	Description
Copy Traveler to device for the following users	Select the users that will have Traveler installed on their machines. Use the **Add** and **Remove** buttons to manage selected users.
Copy Traveler to device for everyone except the following users	Select the users that will be exempt from having Traveler installed. Use the **Add** and **Remove** buttons to manage selected users.

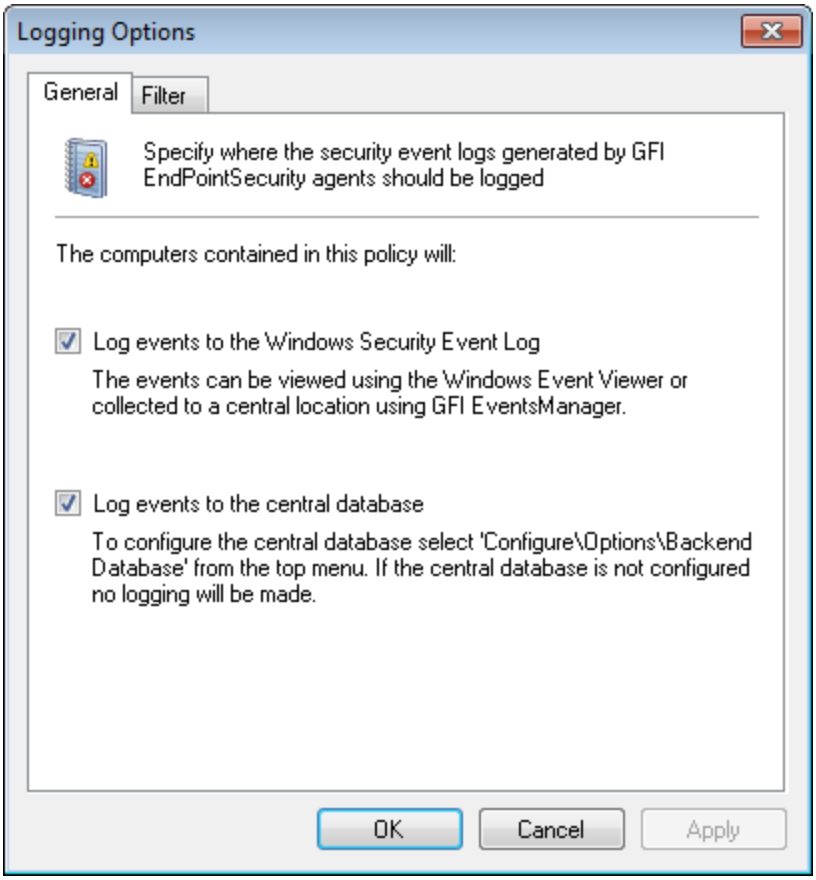
8. Click **Apply** and **OK**.

6.16 Configuring event logging

GFI EndPointSecurity agents record events related to attempts made to access devices and connection ports on target computers. The agents also record events related to service operations. You can specify where these events are to be stored, and also what types of events are to be logged. You can do this on a policy by policy basis.

To specify logging options for users in a protection policy:

1. Click **Configuration** tab > **Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. From the right pane, click **Set Logging Options** in the **Logging and Alerting** section.

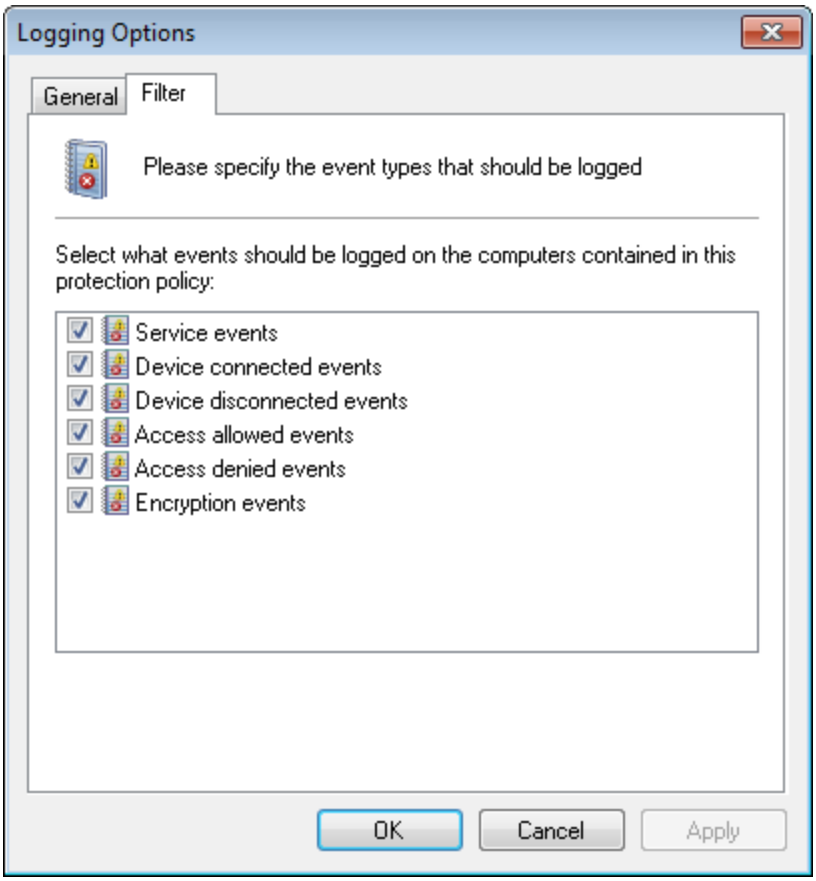


Screenshot 69: Logging Options - General tab

4. In the **Logging Options** dialog, click **General** tab.
5. Enable or disable the locations where to store events generated by this protection policy:

Option	Description
Log events to the Windows Security Event Log	you can view events through the Windows Event Viewer of every target computer or through GFI EventsManager after they are collected in a central location
Log events to the central database	you can view the events within the **Logs Browser** sub-tab in the GFI EndPointSecurity management console. This option requires the configuration of a central database. For more information, refer to Managing the Database Backend (page 126).

If both options are enabled, then the same data is logged in both locations.



Screenshot 70: Logging Options - Filter tab

6. Select **Filter** tab, and select any of the following event types to log by this protection policy. Click **OK**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers**….

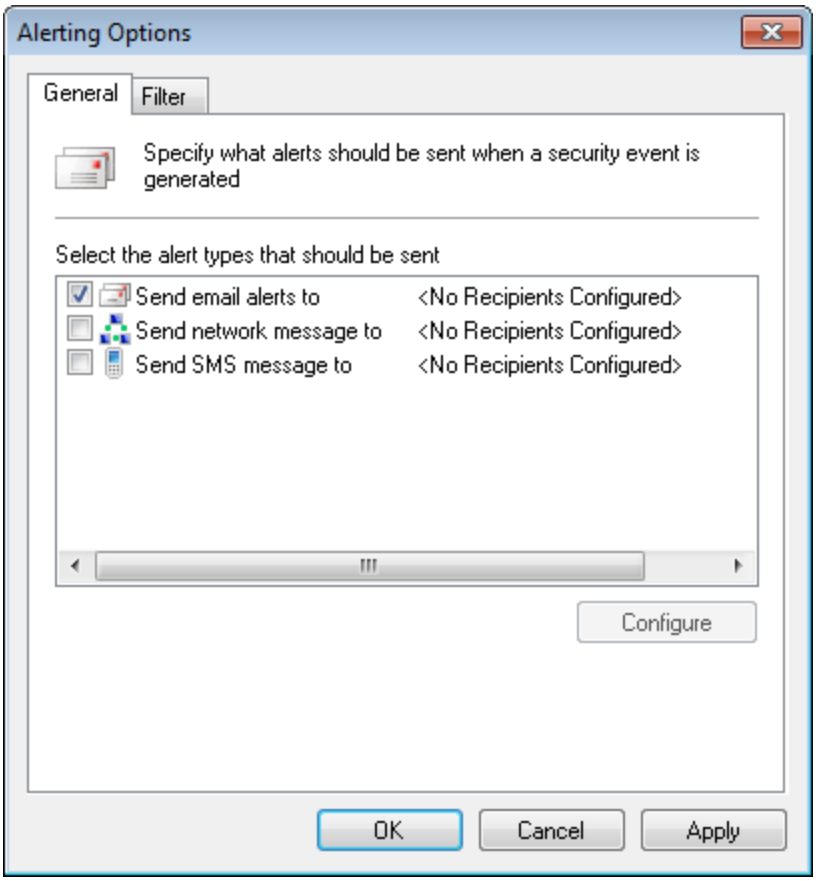
6.17 Configuring alerts

GFI EndPointSecurity can be configured to send alerts to specified recipients when particular events are generated. You can configure alerts to be sent through several alerting options, and also specify the types of events for which alerts are sent. You can do this on a policy by policy basis.

Alert recipients are not Active Directory (AD) users and/or user groups, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts. It is best to create alert recipients prior to configuring alerts. For more information, refer to Configuring alerts recipients (page 135).

To specify alerting options for users in a protection policy:

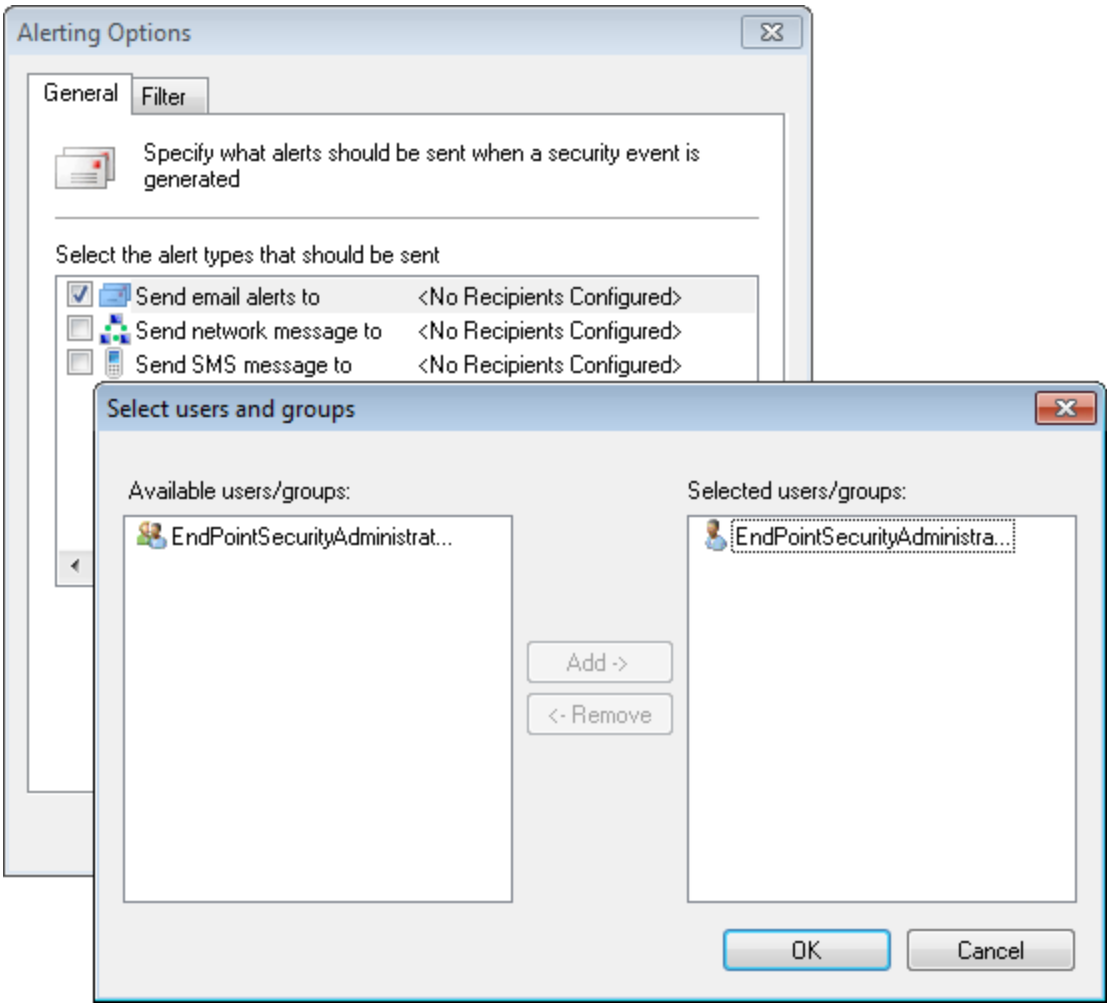
1. Click **Configuration** tab **> Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. From the right pane, click **Alerting options** in the **Logging and Alerting** section.



Screenshot 71: Alerting Options - General tab

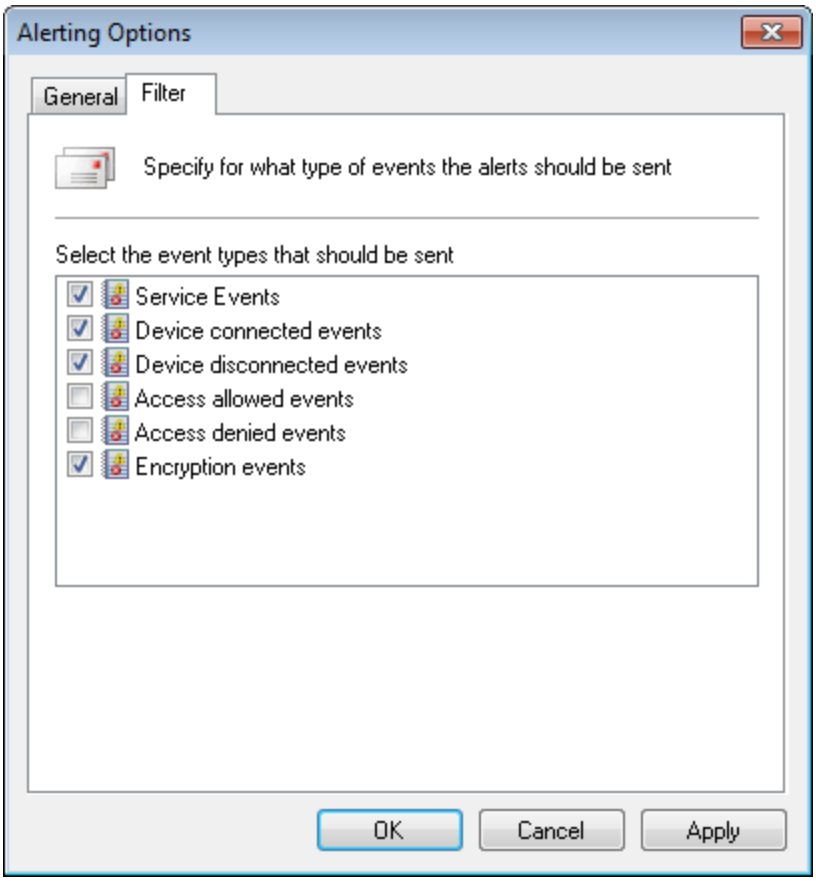
4. In the **Alerting Options** dialog, click **General** tab and select any of the following alert types to send:

- Email alerts
- Network messages
- SMS messages.



Screenshot 72: Alerting Options - Configuring users and groups

5. For each alert type enabled, highlight the alert type and click **Configure** to specify alerts recipients. Click **OK**.



Screenshot 73: Alerting Options - Filter tab

6. Select **Filter** tab, select any of the following event types for which alerts are sent by this protection policy. Click **OK**.

To deploy protection policy updates on target computers specified in the policy:

1. Click **Configuration** tab > **Computers**.
2. From **Common tasks**, click **Deploy to all computers**….

6.18 Setting a policy as the default policy

GFI EndPointSecurity provides you with the facility to define the protection policy that is assigned to newly discovered network computers by the agent deployment feature. You can do this on a policy by policy basis.

By default the agent deployment feature is set to use the **General Control** protection policy, but you can elect any other protection policy as the default policy.

To elect another protection policy as the default protection policy:

1. Click **Configuration** tab **> Protection Policies**.
2. From **Protection Policies > Security**, select the protection policy to configure.
3. From the left pane, click **Set as default policy** in the **Common tasks** section.

7 Discovering Devices

GFI EndPointSecurity enables you to transparently and rapidly query organizational network endpoints, locating and reporting all devices that are or have been connected to the scanned target computers. The application granularly identifies endpoint devices connected to the target computers, both currently and historically, and displays the detailed information on screen once the scan is complete.

Use the **Scanning** tab to scan target computers and discover connected devices. By default, GFI EndPointSecurity scans all supported device categories and connectivity ports.

A discovered target computer can be any computer on the network, and may not be included in any GFI EndPointSecurity protection policy. The device scan must be executed under an account that has administrative privileges over the target computer(s).

Topics in this chapter

7.1 Running a device scan 100

7.2 Analyzing device scan results 103

7.3 Adding discovered devices to the database 104

7.1 Running a device scan

Running a device scan is essential in order to discover new devices. GFI EndPointSecurity enables you to search for new devices that are connected to your target computer. This enables you to add new devices as soon as they are detected on it.

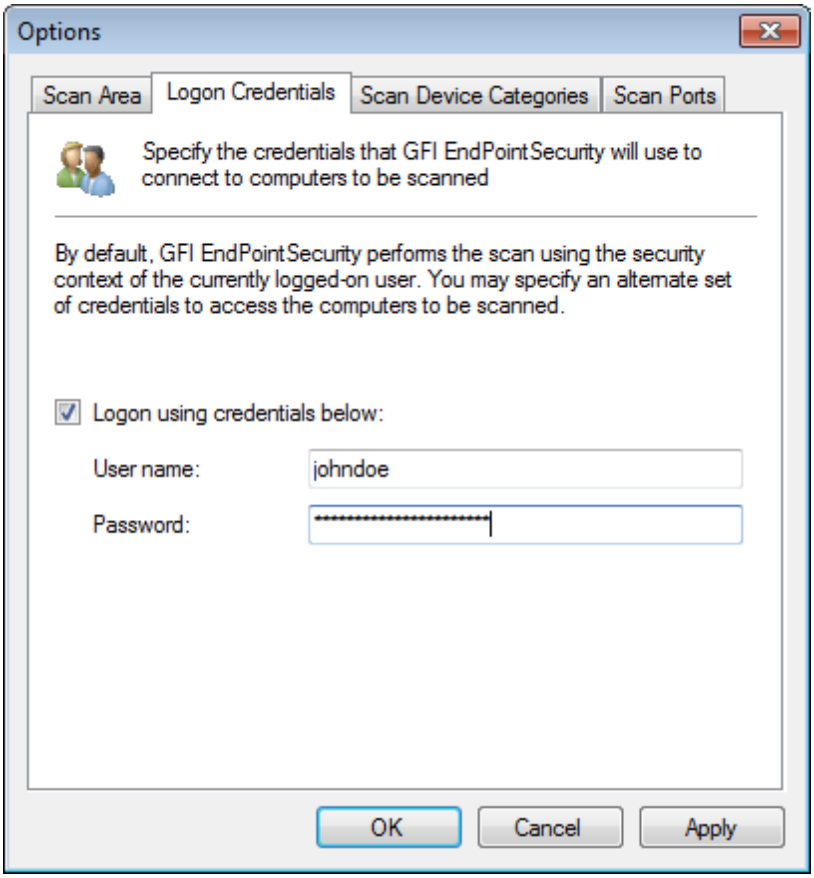
> **Note:**
>
> A new security policy has been introduced in Microsoft Vista, Microsoft Windows 7 and Microsoft Windows 2008 which needs to be enabled in order for the GFI EndPointSecurity device scanner to enumerate the physical devices located on the machine.

To enable remote access to the Plug and play interface:

1. Logon to the Microsoft Windows Vista, 7 or Server 2008 computer with administrative privileges
2. Click **Start** > **Run**.
3. Type in **gpedit.msc**.
4. Browse to **Computer Configuration** > **Administrative Templates** > **System** > **Device Installation**.
5. Right click **Allow remote access to the PnP interface** and select **Properties**.
6. Under the **Settings** tab, select the **Enable** option.
7. Click **Ok** to save changes.
8. Restart the computer.

To run a device scan:

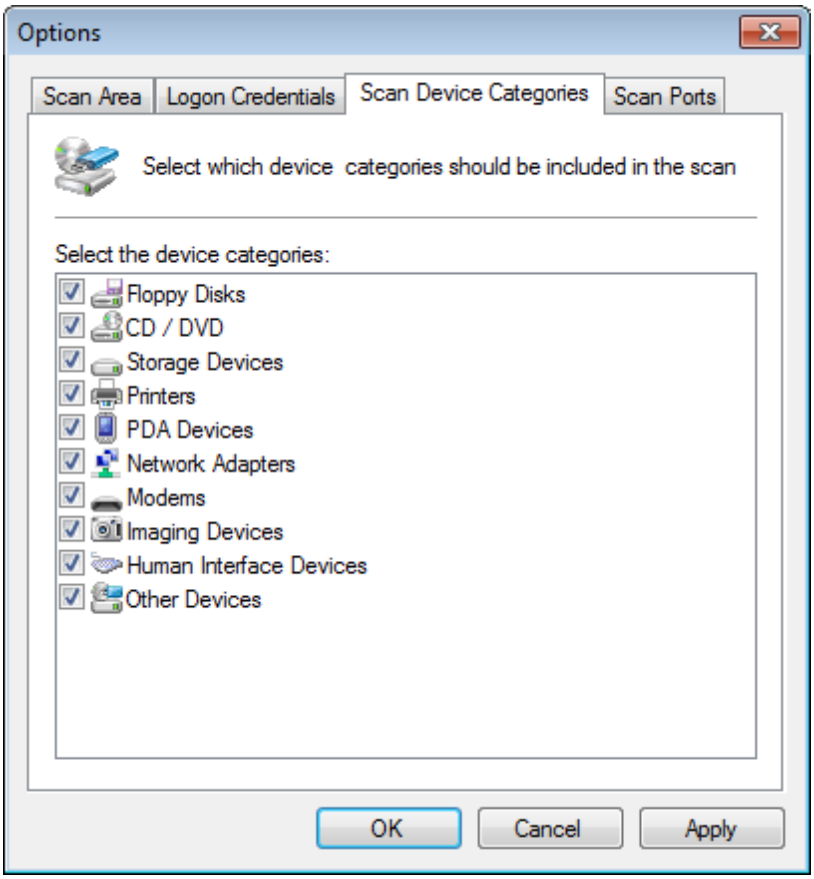
1. Click **Scanning** tab.
2. From **Common tasks**, click **Options**.
3. From the **Options** dialog, select **Logon Credentials** tab.



Screenshot 74: Running a device scan - Logon credentials tab

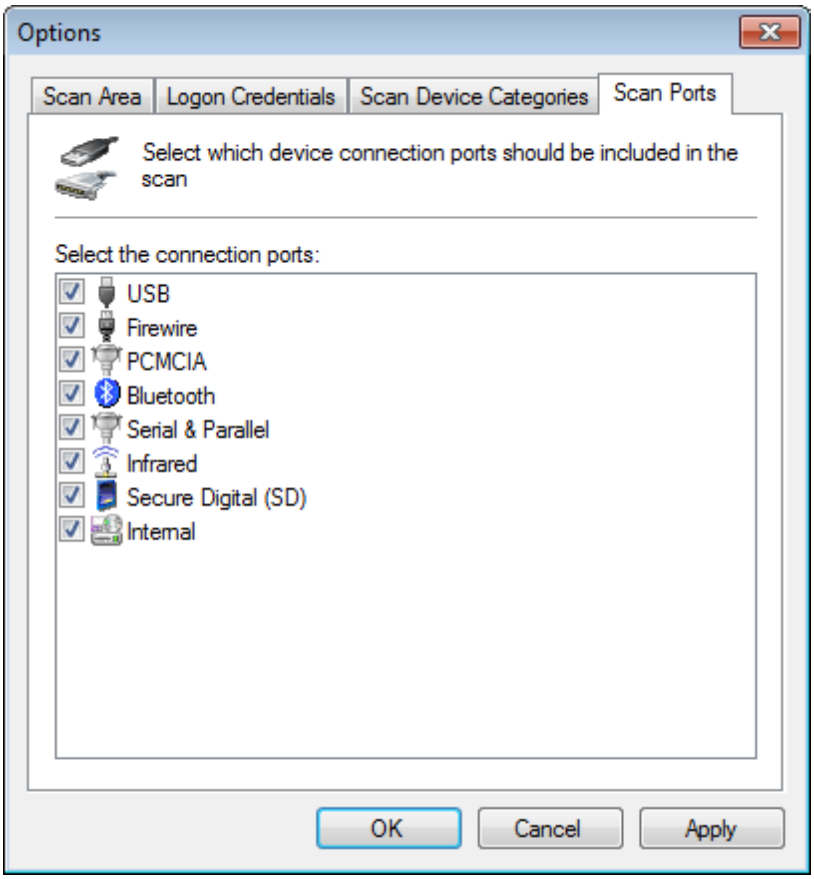
4. From the **Logon Credentials** tab of the **Options** dialog, select/unselect **Logon using credentials below** to enable/disable use of alternate credentials.

> **Note**
>
> If you do not specify any logon credentials, GFI EndPointSecurity attempts to logon the target computer using the currently logged-on user.



Screenshot 75: Running a device scan - Scan device categories tab

5. Click **Scan Device Categories** tab and select the device categories you want to include in the scan.



Screenshot 76: Running a device scan - Scan ports tab

6. Click **Scan Ports** tab and select the connection ports you want to include in the scan.
7. Click **Apply** and **OK**.
8. To specify scan target computers:

» In the right pane, key in the computer name or IP address of the target computer(s) in the **Scan target** text box. Click **New Scan** to start scanning the specified computer.

7.2 Analyzing device scan results

Device Scan results are displayed in two sections:

» Computers

» Devices list.

7.2.1 Computers

Computers:

Computer	User	Protected	Devices	Devices Connected	Version
XP01	TCDOMAINA\administrator	Yes	2	2	4 (20100324)
XP04	TCDOMAINA\Administrator	Yes	2	2	4 (20100324)

Screenshot 77: Computers area

This section displays device scan summary results for every scanned target computer, including:

- The computer name / IP address
- The user currently logged on
- Protection status, i.e., whether the computer is included in a GFI EndPointSecurity protection policy
- Total number of devices currently and historically connected
- Number of devices currently connected.

If a scanned target computer is not included in any GFI EndPointSecurity protection policy, you can choose to deploy a protection policy to the computer. To do this:

1. Right-click on the relevant computer name / IP address under **Computer** column, and select **Deploy agent(s)...**
2. Select the protection policy to deploy. Click **Next** to continue and **Finish** to start deployment.

7.2.2 Devices list

Devices list:

Device Name	Device Description	Connected	Device Category	Connection Port	Vendor ID
Floppy disk drive		Yes	Floppy Disks	Internal	
Msft Virtual CD/ROM		Yes	CD / DVD	Internal	msft

Screenshot 78: Devices list area

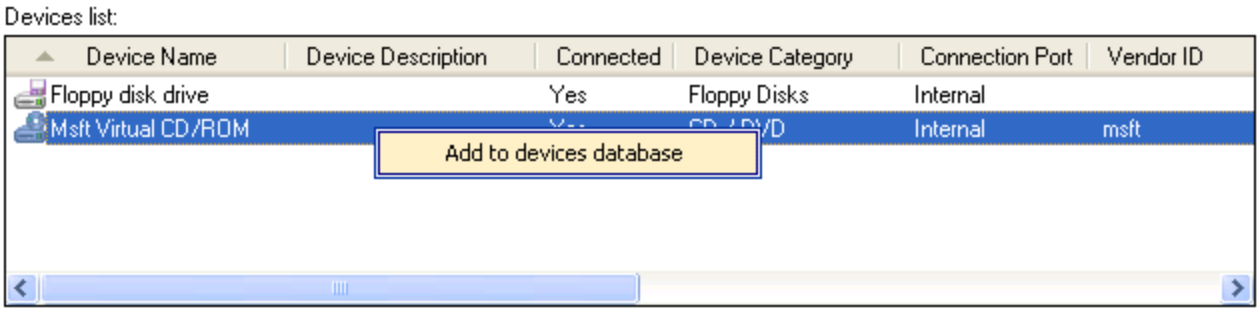
This section displays a detailed list of discovered devices for every scanned computer, including:

- Device name, description and category
- Connectivity port
- Connection status, i.e., whether the device is currently connected or not.

7.3 Adding discovered devices to the database

You can select one or more of the discovered devices from the **Devices** list and add them to the devices database. These devices are then retrieved from this database whenGFI EndPointSecurity

lists the devices currently connected to the target computers for the blacklist and whitelist. For information, refer to Configuring device blacklist or Configuring device whitelist.



Screenshot 79: Devices list area - Add device to devices database

To add devices to the devices database:

1. Select one or more devices to add to the devices database from the **Devices** list section.
2. Right-click on the selected devices and select **Add to devices database**.
3. Click **OK**.

8 Monitoring Device Usage Activity

This chapter provides you with information about monitoring the activity of your network devices. GFI EndPointSecurity enables you to keep an audit trail of all events generated by GFI EndPointSecurity Agents deployed on network computers. To maintain an audit trail, you must enable logging. For more information, refer to Configuring event logging (page 94).

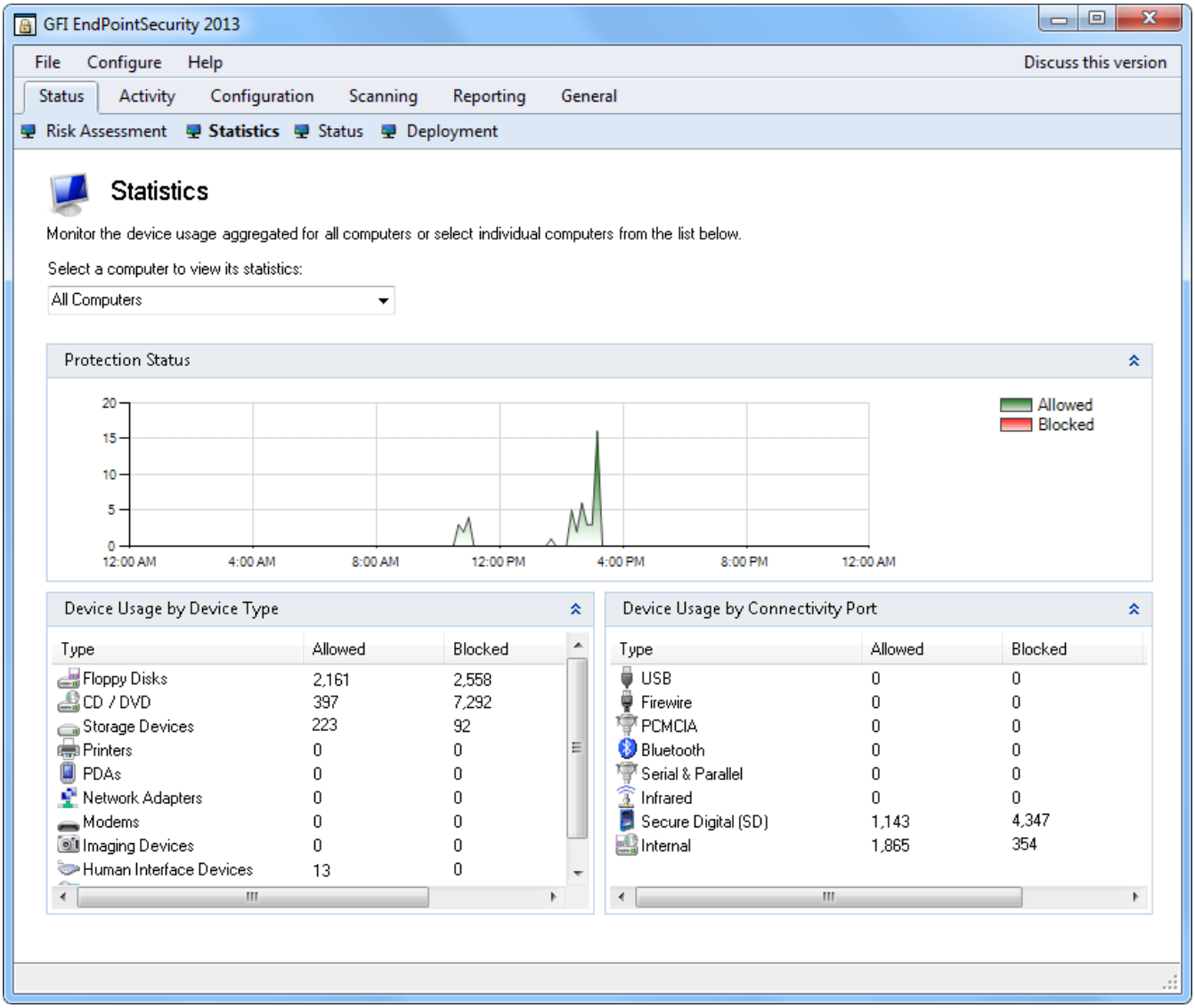
Topics in this chapter

8.1 Statistics 106

8.2 Activity 108

8.1 Statistics

Use the Statistics sub-tab to view the daily device activity trends and statistics for a specific computer or for all network computers.



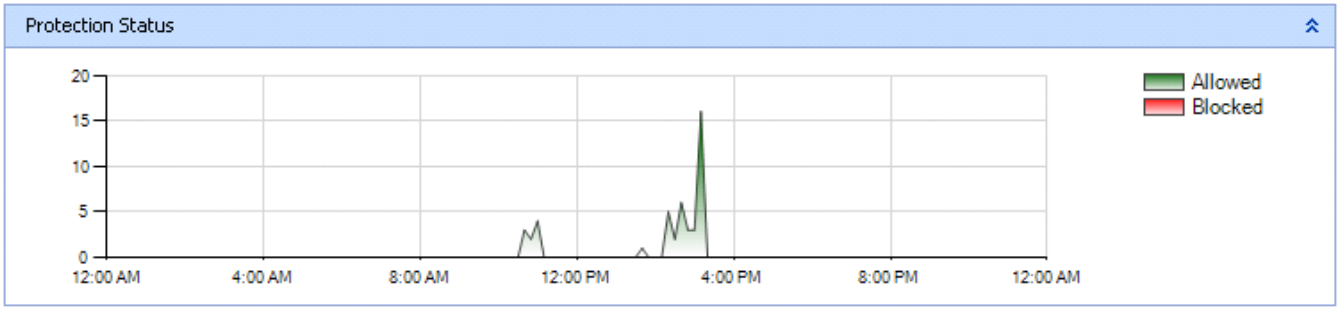
Screenshot 80: Statistics sub-tab

To access the Statistics sub-tab, from GFI EndPointSecurity management console click **Status** tab > **Statistics**.

The **Statistics** section contains information about:

- Protection Status
- Device Usage by Device Type
- Device Usage by Connectivity Port

8.1.1 Protection Status



Screenshot 81: Protection Status area

This section graphically represents daily device usage on computers, differentiating between devices that have been blocked and devices that have been allowed by the agents. The information provided can be filtered for a specific computer or for all network computers.

8.1.2 Device Usage by Device Type

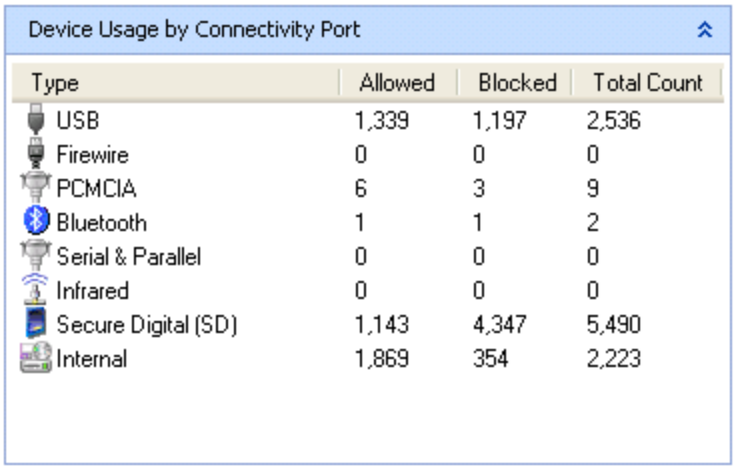
Device Usage by Device Type

Type	Allowed	Blocked	Total Count
Floppy Disks	2	88	90
CD / DVD	2,161	397	2,558
Storage Devices	1,939	5,353	7,292
Printers	11	5	16
PDAs	10	7	17
Network Adapters	16	13	29
Modems	6	5	11
Imaging Devices	5	7	12
Human Interface Devices	4	4	8
Other Devices	200	23	223

Screenshot 82: Device Usage by Device Type area

This section enumerates device connection attempts by device type, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

8.1.3 Device Usage by Connectivity Port



Type	Allowed	Blocked	Total Count
USB	1,339	1,197	2,536
Firewire	0	0	0
PCMCIA	6	3	9
Bluetooth	1	1	2
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	1,143	4,347	5,490
Internal	1,869	354	2,223

Screenshot 83: Device Usage by Connectivity Port area

This section enumerates device connection attempts by connectivity port, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

8.2 Activity

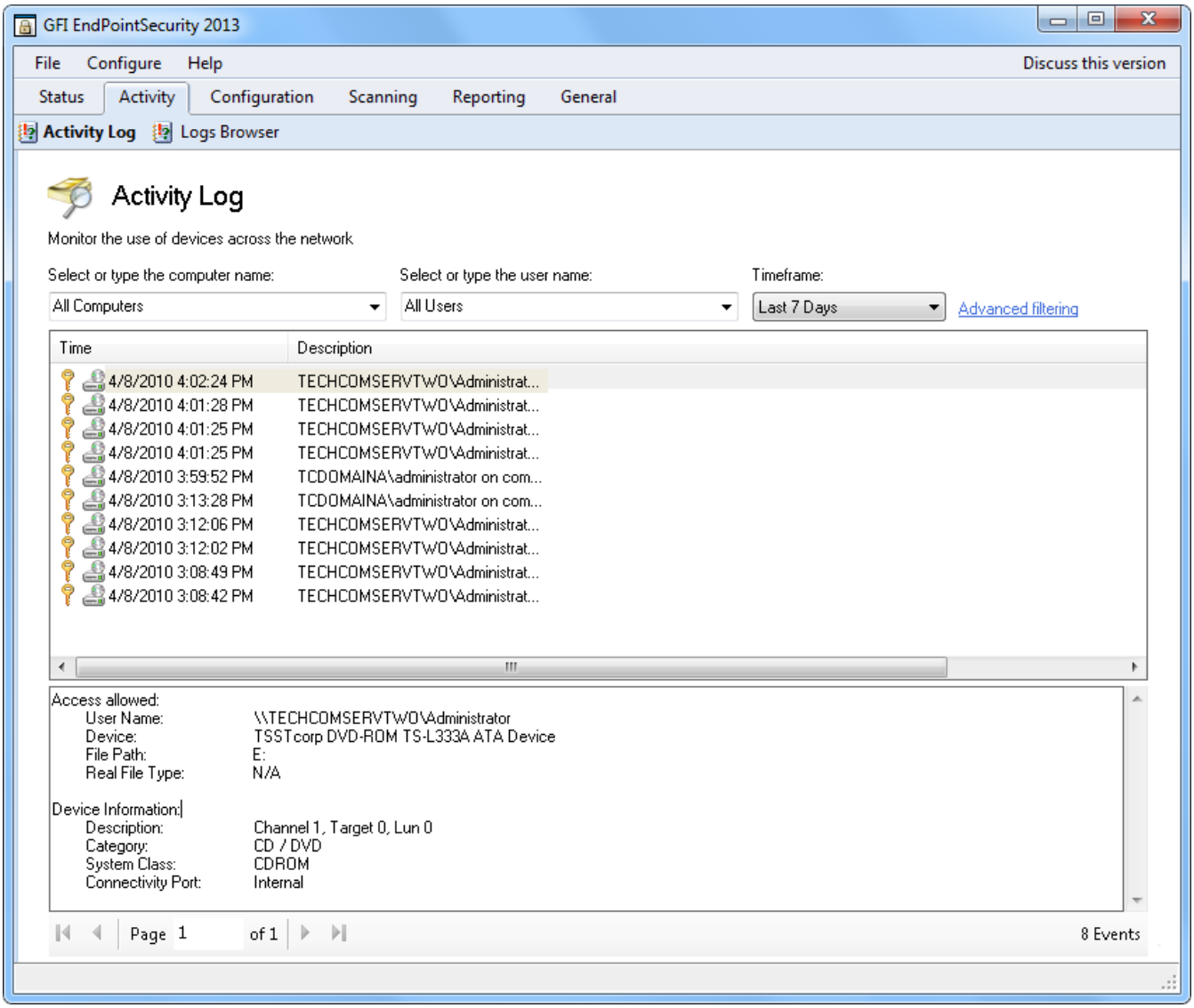
Use the Activity tab to monitor device usage across the network and logged events for a specific computer or for all network computers.

The Activity section contains information about:

- Activity Log
- Advanced Filtering
- Logs Browser
- Creating event queries

8.2.1 Activity Log

This sub-tab allows you to monitor the devices in use on the network. Select the computer and/or user from the relevant drop-down lists to filter the Activity Log list by computer and/or by user. In addition, this tab allows you to further filter down the list by the provided time filters.



Screenshot 84: Activity Log sub-tab

To access the Activity Log sub-tab, from GFI EndPointSecurity management console click **Activity** tab **> Activity Log**.

To view more details about a particular event, click on the event. Additional information is displayed in the events description pane at the bottom of the sub-tab.

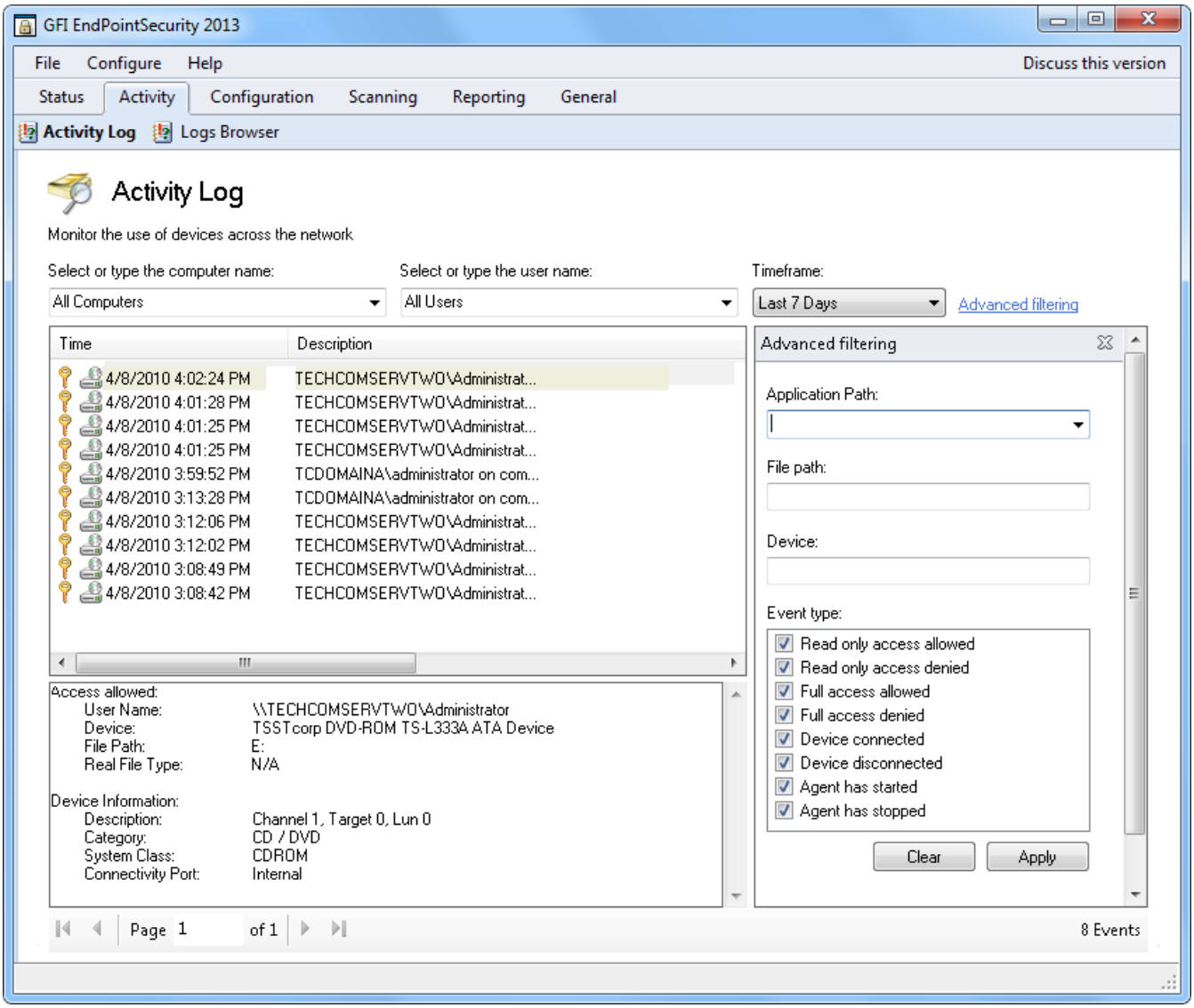
To customize the Activity Log sub-tab to suit your company's needs, right-click the header and select the columns that should be added to or removed from the view.

To change a column's position, select the column header, drag and drop it at the required position.

8.2.2 Advanced Filtering

This feature allows you to further filter down the device usage history logs using one or more criteria from the following set:

- Application Path
- File path
- Device
- Event type.



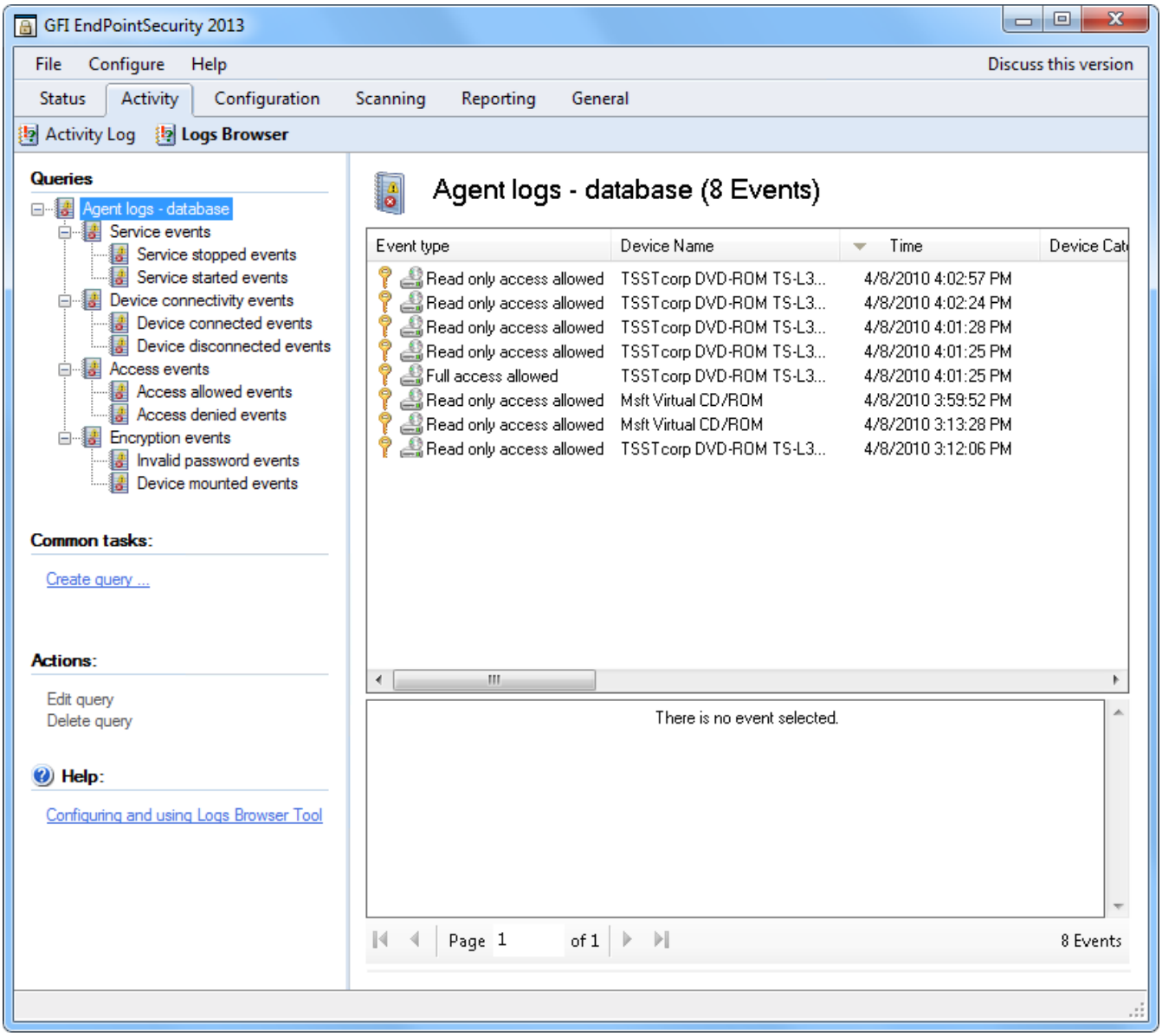
Screenshot 85: Activity Log sub-tab - Advanced filtering

To access advanced filtering options of Activity Log, click **Advanced filtering** in the **Activity Log** sub-tab.

8.2.3 Logs Browser

The Logs Browser sub-tab allows you to access and browse events currently stored in the database backend.

GFI EndPointSecurity also includes a query builder to simplify searching for specific events. With the events query builder you can create custom filters that filter events data and display only the information that you need to browse - without deleting records from your database backend.



Screenshot 86: Logs Browser sub-tab

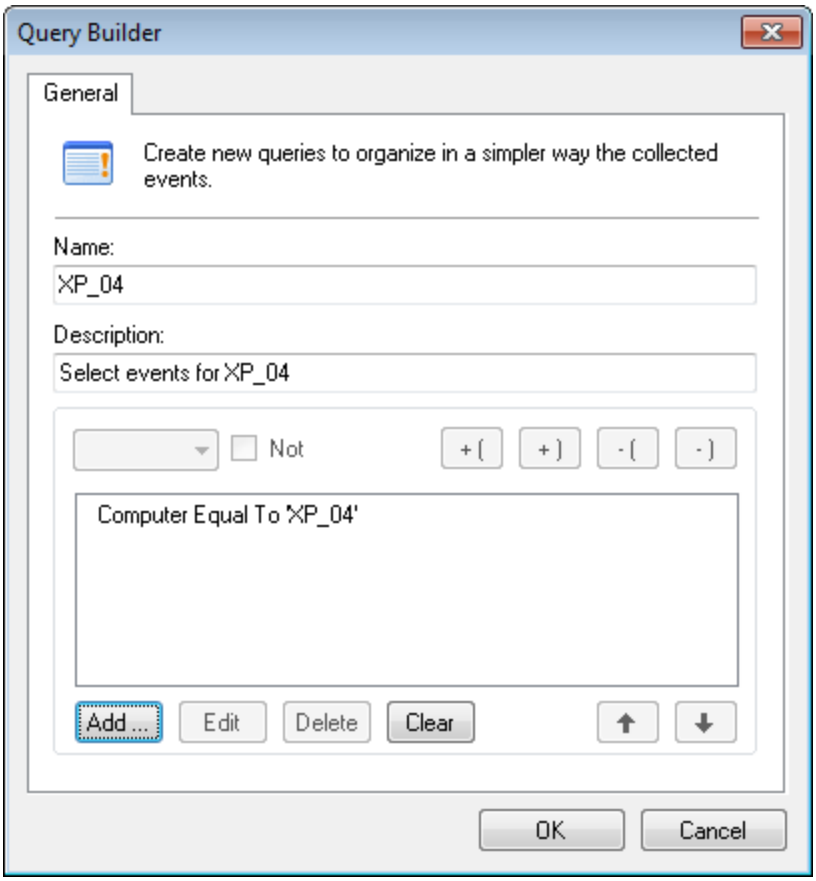
To access the Logs Browser sub-tab, from GFI EndPointSecurity management console click **Activity** tab > **Logs Browser**.

To view more details about a particular event, click on the event. Additional information is displayed in the events description pane at the bottom of the sub-tab.

8.2.4 Creating event queries

To create custom event queries:

1. From GFI EndPointSecurity management console, click **Activity** tab.
2. Click **Logs Browser** sub-tab.
3. In the left pane, right-click **Agent logs - database** node and select **Create query…**.



Screenshot 87: Query Builder options

4. In the **Query Builder** dialog, specify a name and a description for the new query.
5. Click **Add…**, configure the required query condition(s) and click **OK**. Repeat until all required query conditions have been specified.
6. Click **OK** to finalize your settings. The custom query is added as a sub-node within **Agent logs - database** node.

> **Note**
>
> You can also filter the results of existing event queries by creating more specific sub-queries. To do this right-click on a query and select **Create query…**.

9 Status Monitoring

This chapter provides with information related to monitoring the status of GFI EndPointSecurity as well as the status of GFI EndPointSecurity Agents. The status views provide you with graphs and statistical information related to device usage.

Topics in this chapter

9.1 Risk Assessment view 113

9.2 Statistics view 115

9.3 Status view 117

9.4 Deployment status view 119

9.1 Risk Assessment view

Use the Risk Assessment sub-tab to view the status of:

- Risk assessment level on the network computers with GFI EndPointSecurity agents installed on them.
- GFI EndPointSecurityagents deployed on network computers.
- Device usage such as the number and percentage of devices blocked and the number of devices allowed.
- Device threat level of devices on the network.

Screenshot 88: Risk Assessment sub-tab

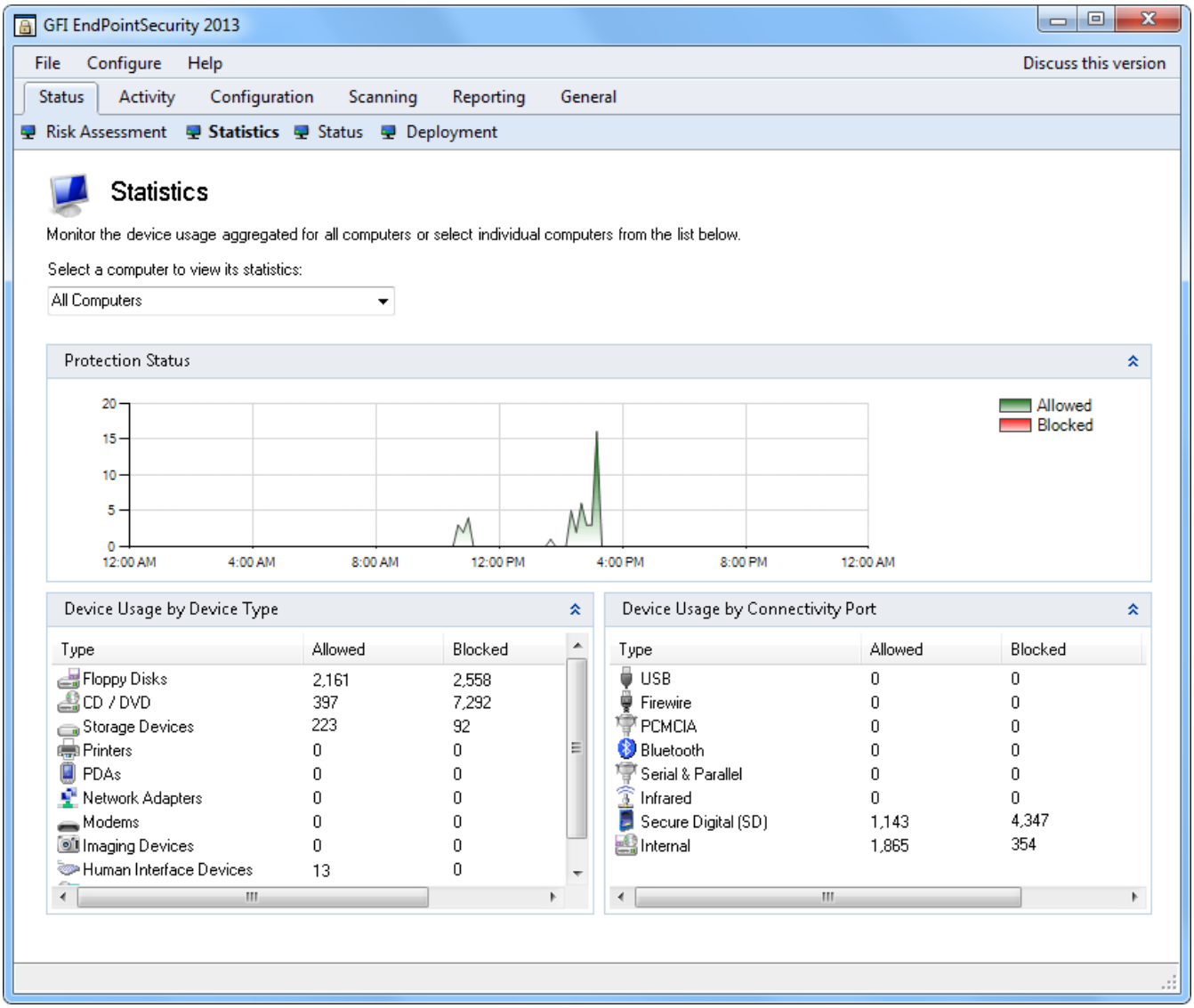
To access the Risk Assessment sub-tab, from GFI EndPointSecurity management console click **Status** tab **>** **Risk Assessment.**

Feature	Description
1	This section shows: » The gauge showing risk assessment results of the network computers. » The option to re-scan the network to obtain the latest risk assessment results. » The Time of the last risk assessment.

Feature	Description
2	This section lists the cumulative values of the number of: » Scanned endpoints » Successful scans » Protected endpoints » Unprotected endpoints » Devices discovered This section also represents: » The network where agents are installed » The time and date of the last risk assessment.
3	This section graphically represents the number of agents that are currently: » Awaiting installation on network computers » Protected by GFI EndPointSecurity » Not protected by GFI EndPointSecurity
4	This section represents all agents deployed on network computers, differentiating between those currently online and those that are offline. For more information, refer to Status view (page 117).
5	This section graphically represents the device threat percentage levels as logged by the agents of network computers that have GFI EndPointSecurityinstalled on them.
6	This section graphically represents the percentages of user accesses per device category of the total cumulative amount of user accesses to devices, as logged by the agents. User accesses to devices refer to both allowed and blocked device accesses.
7	This section lists: » The user account under which the GFI EndPointSecurity service is running. » The risk factor level. » The current encryption status on the endpoint. » The file type checking feature status. » The content checking feature status.

9.2 Statistics view

Use the Statistics sub-tab to view the daily device activity trends and statistics for a specific computer or for all network computers.



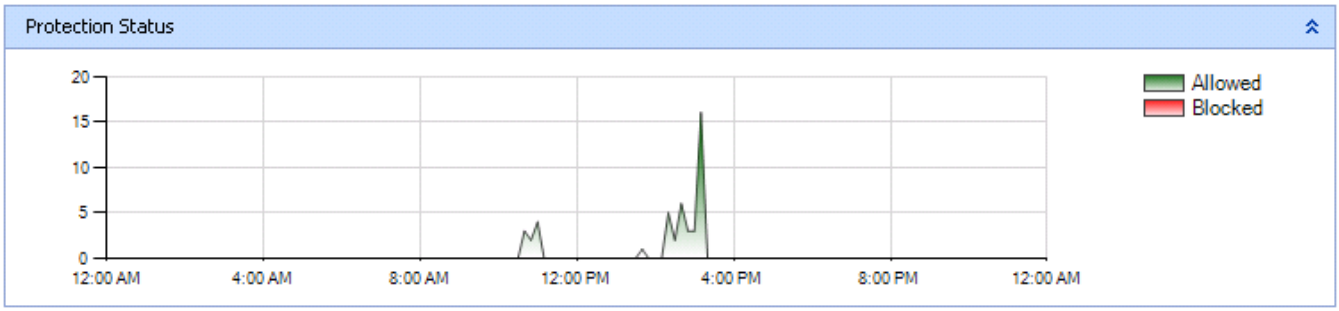
Screenshot 89: Statistics sub-tab

To access the Statistics sub-tab, from GFI EndPointSecurity management console click **Status** tab > **Statistics**.

The **Statistics** section contains information about:

- Protection Status
- Device Usage by Device Type
- Device Usage by Connectivity Port

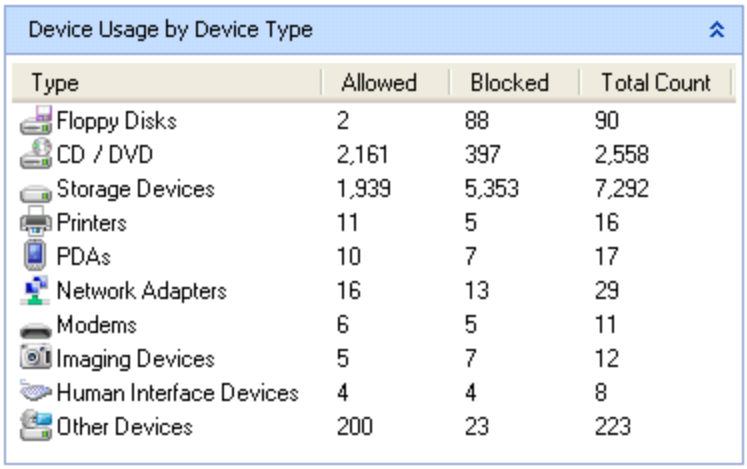
9.2.1 Protection Status



Screenshot 90: Protection Status area

This section graphically represents daily device usage on computers, differentiating between devices that have been blocked and devices that have been allowed by the agents. The information provided can be filtered for a specific computer or for all network computers.

9.2.2 Device Usage by Device Type

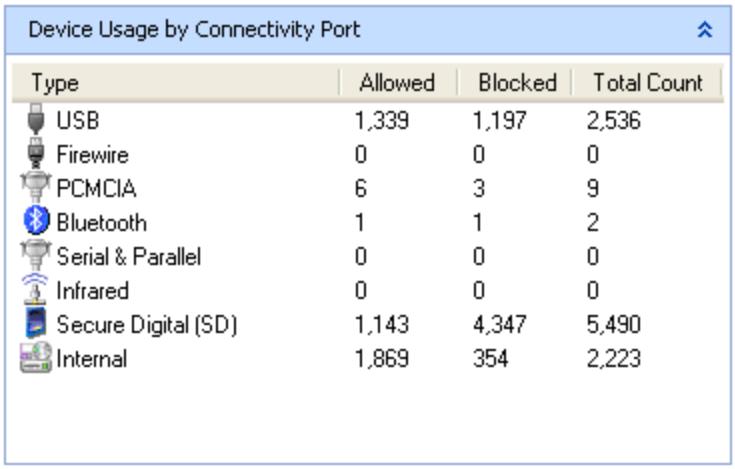

Device Usage by Device Type

Type	Allowed	Blocked	Total Count
Floppy Disks	2	88	90
CD / DVD	2,161	397	2,558
Storage Devices	1,939	5,353	7,292
Printers	11	5	16
PDAs	10	7	17
Network Adapters	16	13	29
Modems	6	5	11
Imaging Devices	5	7	12
Human Interface Devices	4	4	8
Other Devices	200	23	223

Screenshot 91: Device Usage by Device Type area

This section enumerates device connection attempts by device type, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

9.2.3 Device Usage by Connectivity Port


Device Usage by Connectivity Port

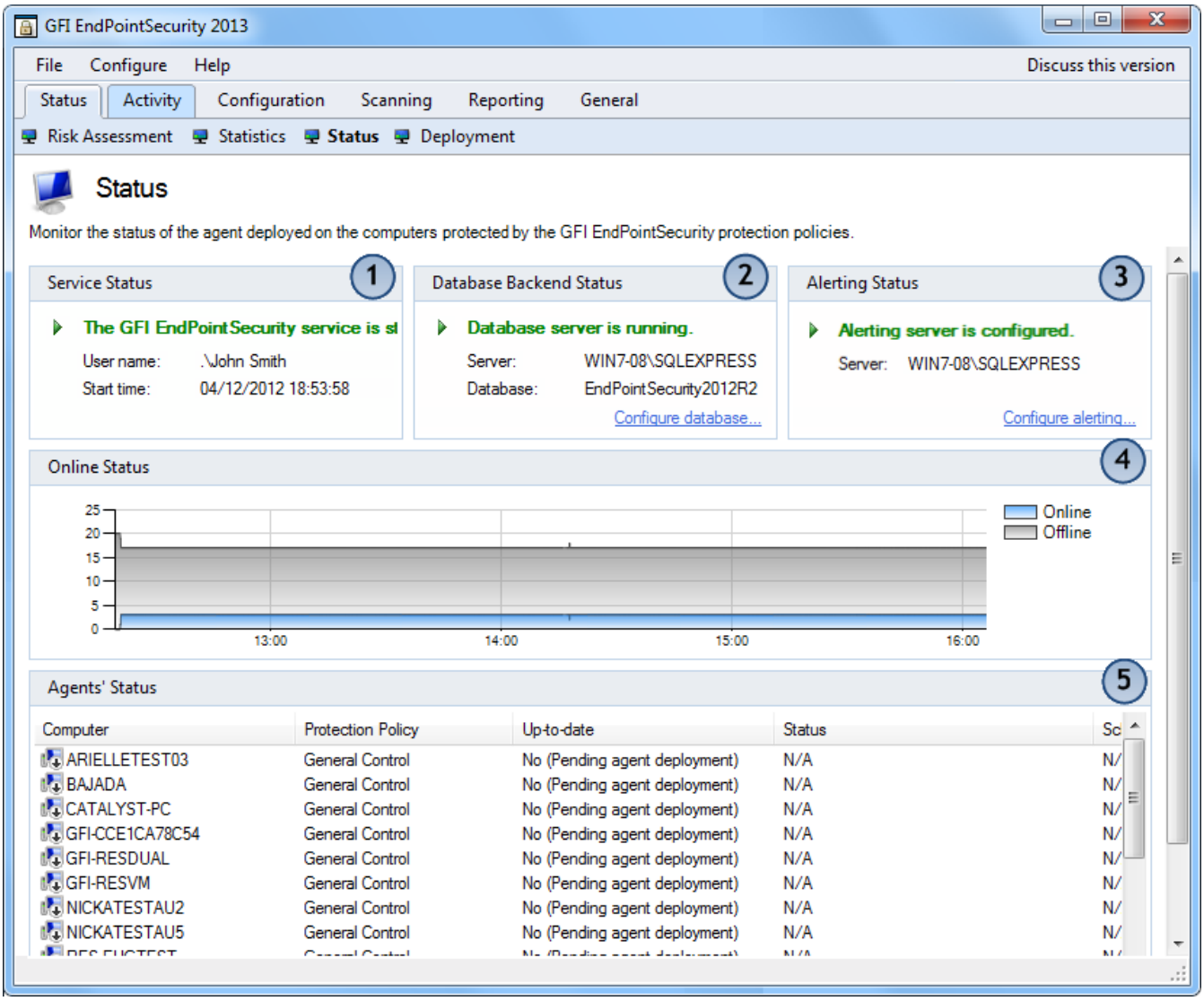
Type	Allowed	Blocked	Total Count
USB	1,339	1,197	2,536
Firewire	0	0	0
PCMCIA	6	3	9
Bluetooth	1	1	2
Serial & Parallel	0	0	0
Infrared	0	0	0
Secure Digital (SD)	1,143	4,347	5,490
Internal	1,869	354	2,223

Screenshot 92: Device Usage by Connectivity Port area

This section enumerates device connection attempts by connectivity port, that were either allowed or blocked. The information provided can be filtered for a specific computer or for all network computers.

9.3 Status view

Use the Status sub-tab to determine the status of all deployment operations performed on your network targets. For each target computer, information displayed shows:



Screenshot 93: Status sub-tab

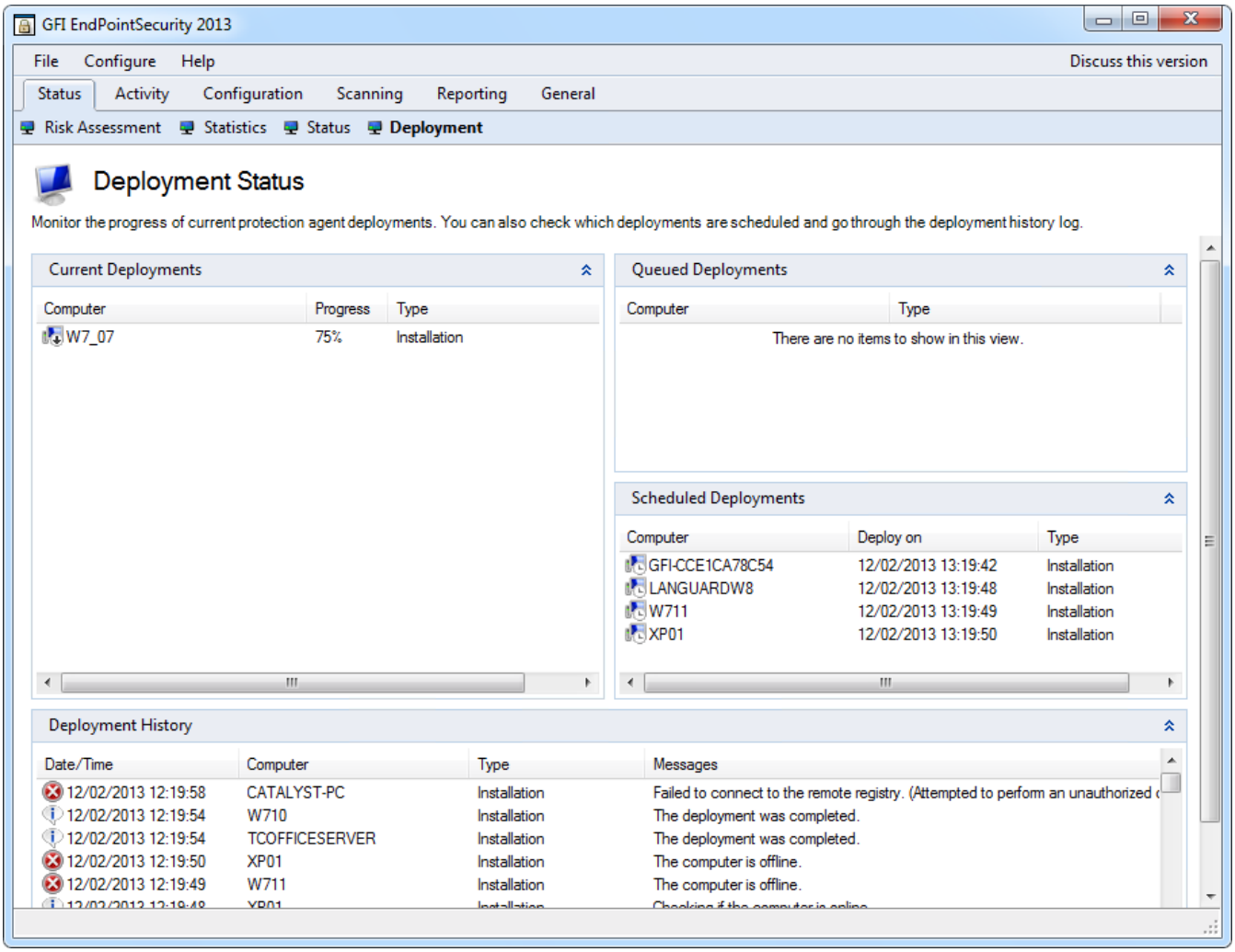
Feature	Description
1	This section lists: » The operational status of GFI EndPointSecurity management console service. » The user account under which the GFI EndPointSecurity service is running. » The time when the service was last started.
2	This section lists: » The operational status of the database server currently used by GFI EndPointSecurity . » The name or IP address of the database server currently used by GFI EndPointSecurity. » The name of the database where GFI EndPointSecurity is archiving events. To modify any of the current database settings, click **Configure database…**. This launches the **Database Backend** dialog. For more information, refer to Managing the Database Backend (page 126).
3	This section lists: » The operational status of the alerting server currently used by GFI EndPointSecurity. » The name or IP address of the alerting server currently used by GFI EndPointSecurity. To modify any of the current alerts related settings, click **Configure alerting** …. This launches the **Alerting Options** dialog. For more information, refer to Configuring alerts (page 96).

Feature	Description
4	This section graphically represents all agents deployed on network computers, differentiating between those currently online and offline.
5	This selection lists: » Target computer name and applicable protection policy. » The status of the GFI EndPointSecurity Agent, whether currently deployed and up-to-date, or awaiting deployment. » The status of the target computer, whether currently online, or offline. To deploy pending agents: 1. Select one or more computers from **Agents' Status**. 2. Right-click the selected computers and select **Deploy selected agent(s)** or **Schedule deployment for selected agent(s)**.... 3. Click **OK**. **Note** If a target computer is offline, deployment is differed by an hour. GFI EndPointSecurity tries to deploy that policy every hour, until the target computer is back online. **Note** Each agent sends its online status to GFI EndPointSecurity at regular intervals. If this data is not received by the main application, the agent is considered to be offline.

9.4 Deployment status view

- About Deployment status view
- Current Deployments
- Queued Deployments
- Scheduled Deployments
- Deployment History

9.4.1 About Deployment status view



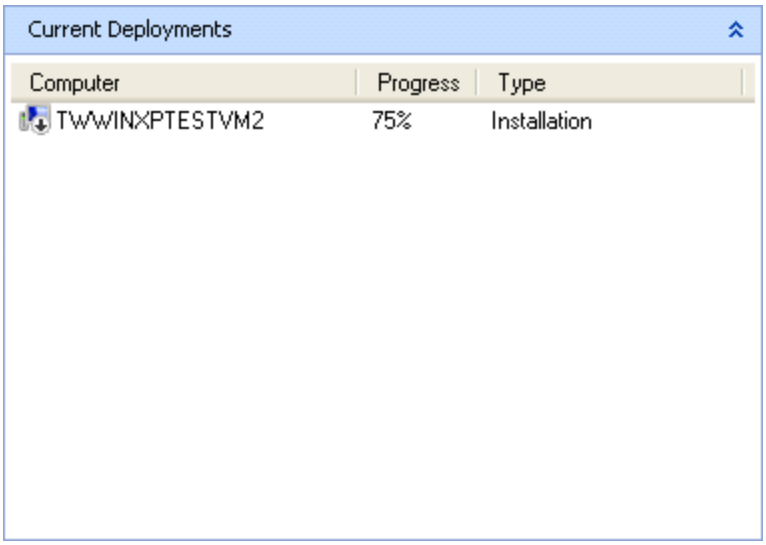
Screenshot 94: Deployment sub-tab

Use the Deployment sub-tab to view:

- Current deployment activity
- Queued deployments
- Scheduled deployments
- Deployment history.

To access the Deployment sub-tab, from GFI EndPointSecurity management console, click **Status** tab **> Deployment**.

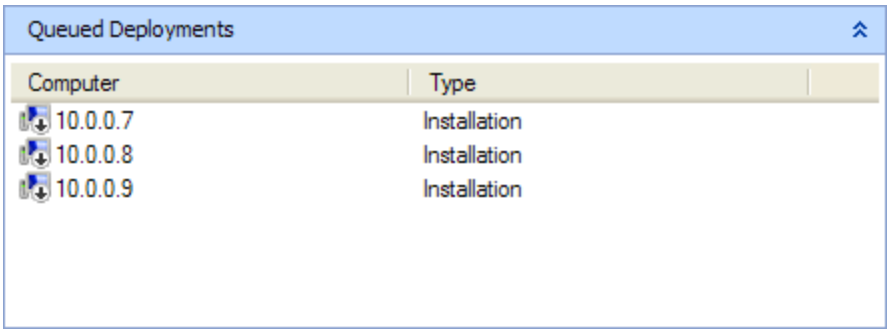
9.4.2 Current Deployments



Screenshot 95: Current Deployments area

This section displays a list of deployments currently taking place. The information provided includes the computer name, deployment progress and deployment type. The deployment is an installation, un-installation or update.

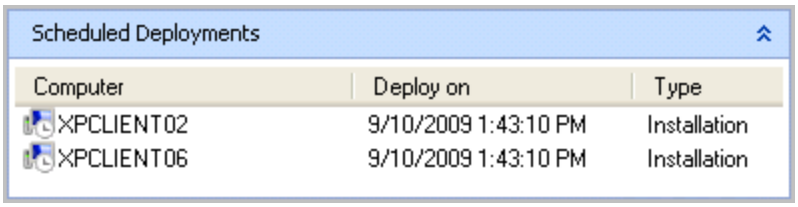
9.4.3 Queued Deployments



Screenshot 96: Queued Deployments area

This section displays a list of pending deployments. The information provided includes the computer name and deployment type.

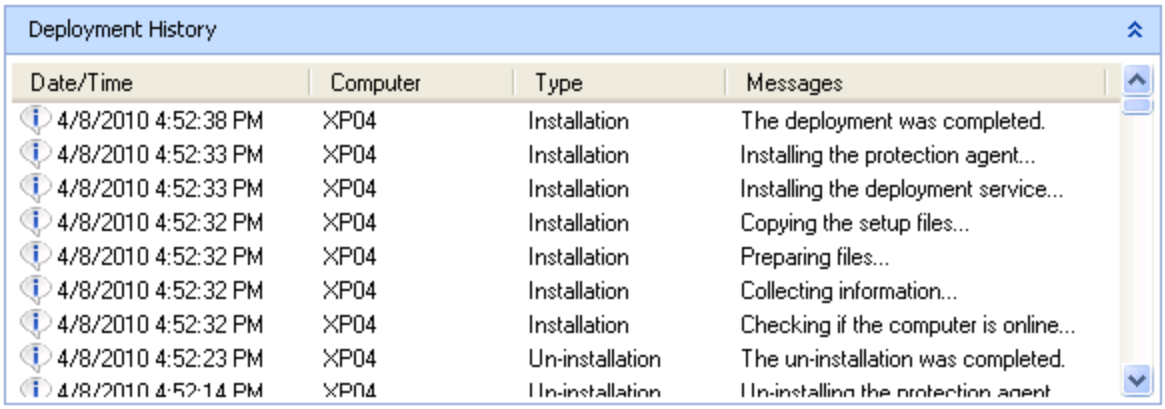
9.4.4 Scheduled Deployments



Screenshot 97: Scheduled Deployments area

This section displays a list of scheduled deployments. The information provided includes the computer name, scheduled time and deployment type.

9.4.5 Deployment History



Screenshot 98: Deployment History area

This section displays an audit trail for all stages of all agent or protection policy deployments carried out by GFI EndPointSecurity. The information provided includes the timestamp of each log entry, the computer name, deployment type and errors and information messages generated during the deployment process. For more information, refer to Troubleshooting and Support (page 147).

To remove displayed log entries, right-click in the **Deployment History** area and select **Clear all messages**.

10 Reporting

The GFI EndPointSecurity GFI ReportPack is a fully-fledged reporting add-on to GFI EndPointSecurity. This reporting package can be scheduled to automatically generate graphical IT-level and management reports based on data collected by GFI EndPointSecurity, giving you the ability to report on devices connected to the network, device usage trends by machine or by user, files copied to and from devices (including actual names of files copied) and much more.

Topics in this chapter

10.1 GFI EndPointSecurity GFI ReportPack 123

10.2 Generating Digest reports 123

10.1 GFI EndPointSecurity GFI ReportPack

To generate reports, you need to download and install the GFI EndPointSecurity GFI ReportPack add-on. To download the add-on visit:http://www.gfi.com/endpointsecurity/esecreportpack.htm

For more information about GFI EndPointSecurity GFI ReportPack:

1. Click **Reporting** tab.
2. From the left pane, select either **GFI EndPointSecurityGFI ReportPack** or **GFI ReportCenter**.

> **Note**
>
> An Internet connection is required.

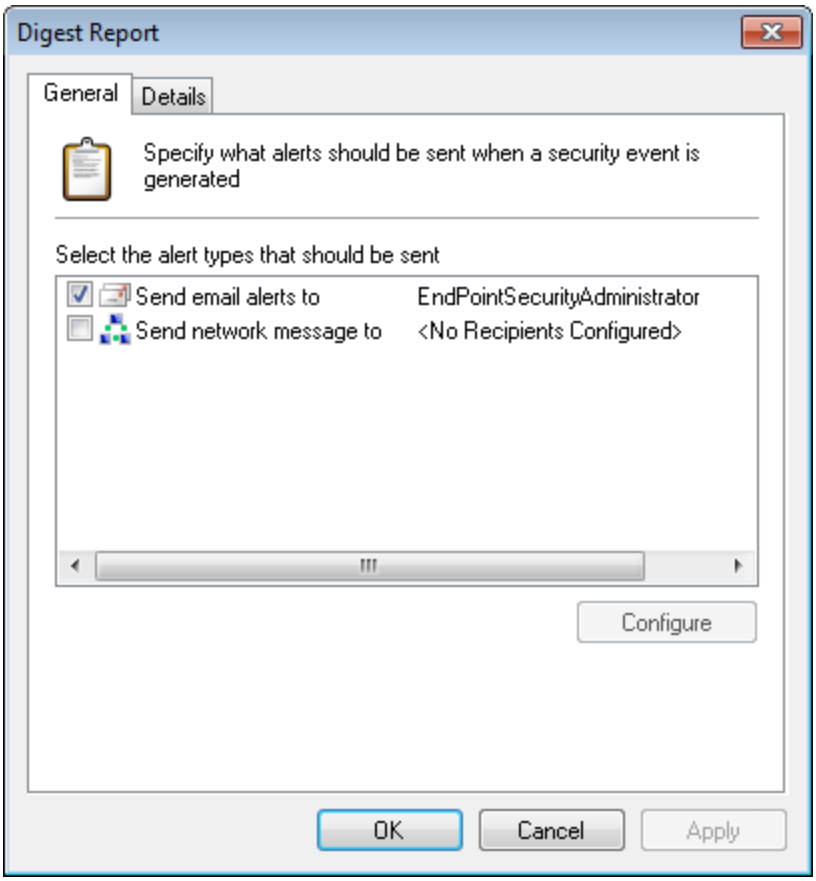
10.2 Generating Digest reports

GFI EndPointSecurity enables you to generate Digest reports to the configured recipients. Digest reports contain a summary of periodical activity statistics as detected by GFI EndPointSecurity.

Alert recipients are not Active Directory (AD) users and/or user groups, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts. It is best to create alert recipients prior to configuring alerts. For more information, refer to Configuring alerts recipients (page 135).

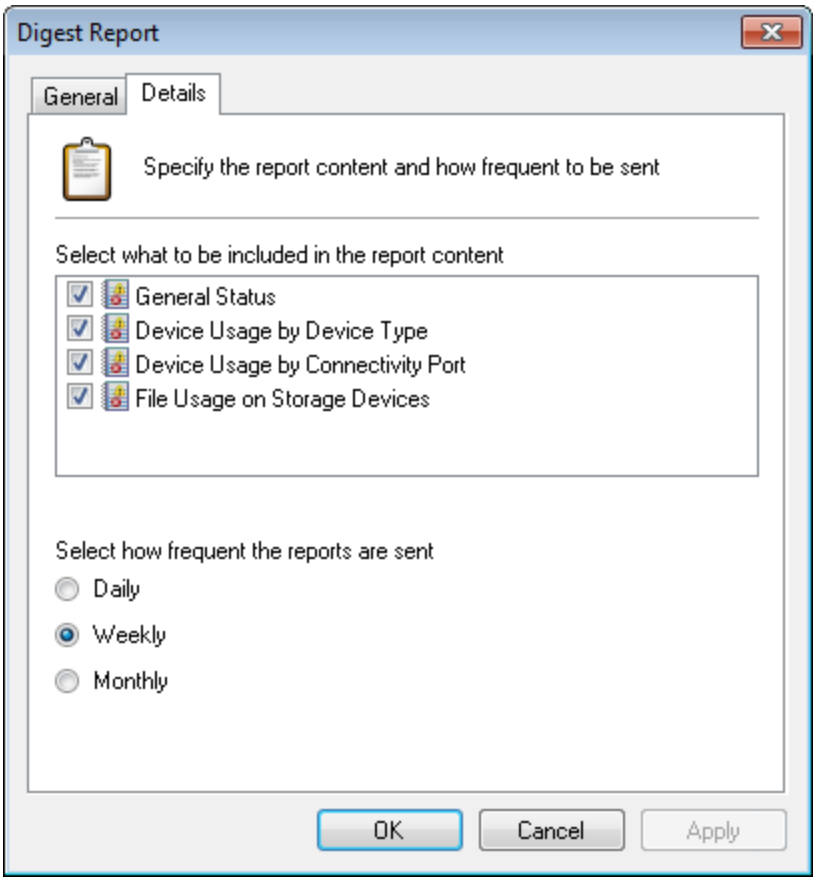
To configure Digest reports:

1. Click **Configuration** tab **>** **Options** sub-tab.
2. From **Configure**, click **Alerting Options** and from the right pane, click **Configure the digest report**.



Screenshot 99: Digest Report options - General tab

3. From the **General** tab of the **Digest Report** dialog, select/unselect the preferred alerting method.
4. For each alert type selected, click **Configure** to specify the user(s)/group(s) to whom the alert is sent.



Screenshot 100: Digest Report options - Details tab

5. Click **Details** tab to select/unselect report content items to include in the digest report.
6. Select the sending frequency of the report, from **Daily**, **Weekly** or **Monthly**.
7. Click **Apply** and **OK**.

11 Managing the Database Backend

This chapter provides you information related to managing and maintaining the database where data gathered by GFI EndPointSecurity is stored. After installing GFI EndPointSecurity you can choose to:

- Download and install an instance of Microsoft SQL Server Express Edition and to automatically create a database for GFI EndPointSecurity. This can be done through the **Quick Start wizard**.
- Connect to an available Microsoft SQL Server instance and connect to an existing database or else create a new one. This can be done through the **Quick Start wizard**, the **General Status** or the **Options** sub-tabs.

Topics in this chapter

11.1 Maintaining the database backend 126

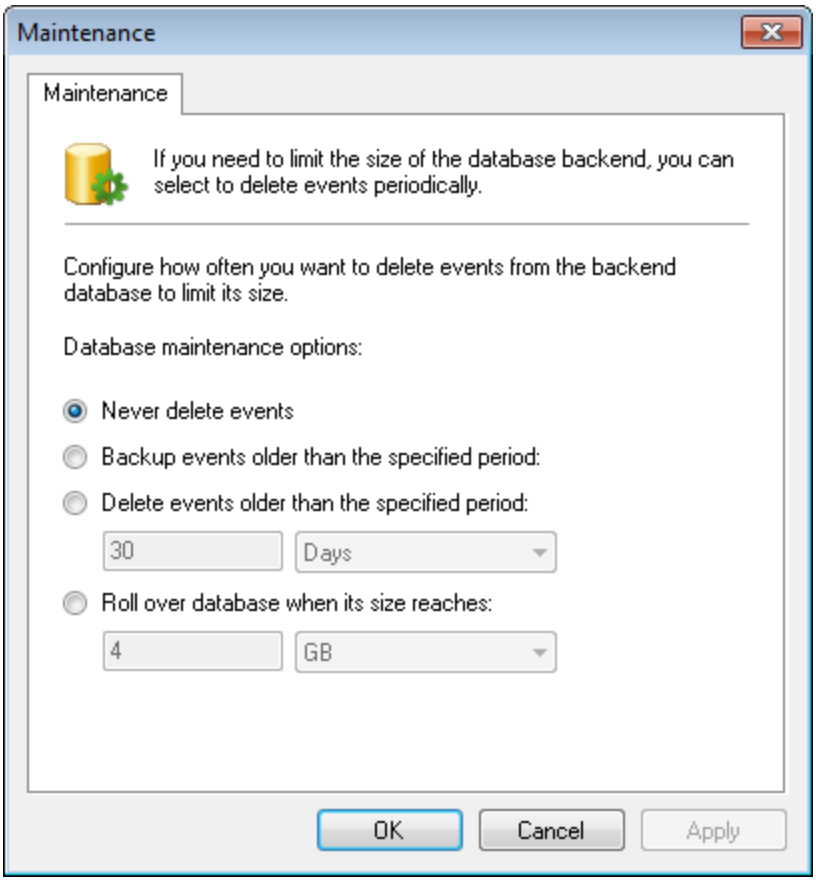
11.2 Using an existing SQL Server instance 128

11.1 Maintaining the database backend

Periodical database maintenance is essential in order to prevent your database backend from growing too much. GFI EndPointSecurity provides you with the facility to configure parameters that automatically maintain your database backend.

To configure database backend maintenance:

1. Click **Configuration** tab > **Options** sub-tab.
2. From **Configure**, select **Database Backend**.
3. From the right pane, click **Database maintenance**.



Screenshot 101: Maintenance options

4. From the **Maintenance** dialog, configure how often events are deleted from the database backend. Select from the options described below:

Table 17: Database maintenance options

Option	Description
Never delete events	Keep all events in your database backend, without deleting old ones. **Note** Ensure that manual deletion of old records is done to prevent GFI EndPointSecurity performance loss.
Backup events older than the specified period	Select this option and specify how old events have to be before they are backed up in a separate database.
Delete events older than the specified period	Select this option and specify how old events have to be before they are deleted.
Roll over database when its size reaches	Specify the maximum size a database can grow before GFI EndPointSecurity automatically switches to a new database.

5. Click **Apply** and **OK**.

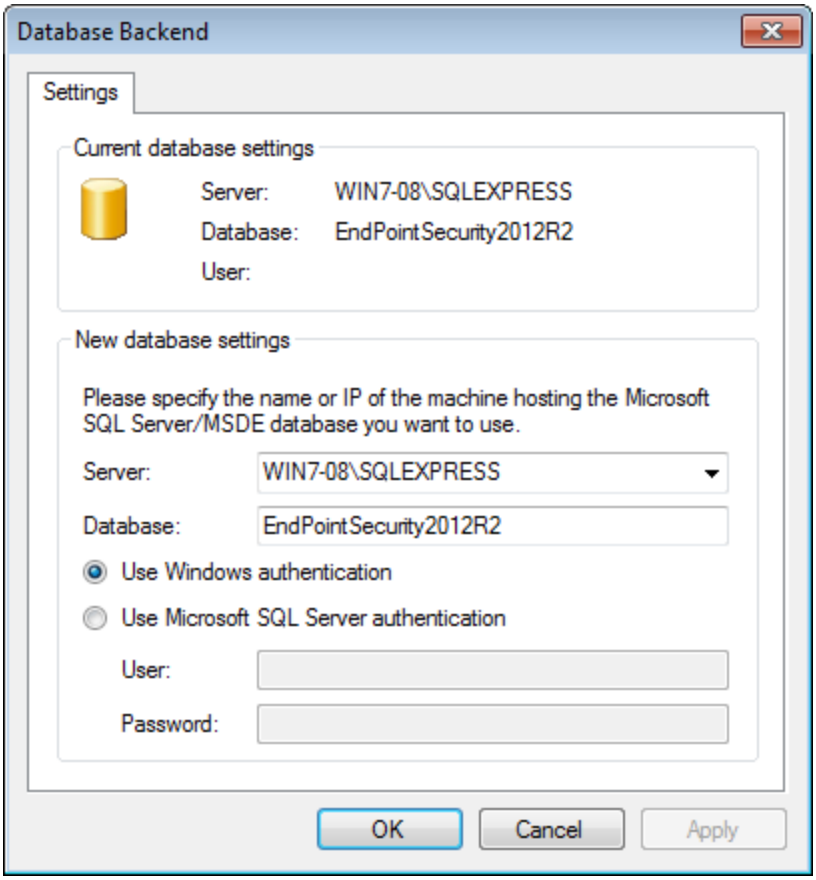
Note

Since Microsoft SQL Express 2005 has a database size limitation of 4 GB and Microsoft SQL Express 2008 R2 has a database limitation of 10 GB, it is recommended to use Roll over database option. For more information on Microsoft SQL Server Edition, engine specifications, refer to http://go.gfi.com/?pageid=ESEC_SqlSpecs

11.2 Using an existing SQL Server instance

To connect to an existing SQL Server instance:

1. Click **Configuration** tab > **Options** sub-tab.
2. From **Configure**, select **Database Backend**.
3. From the right pane, click **Change database backend**.



Screenshot 102: Change Database Backend

4. From the **Server** drop-down menu, select the SQL Server you want to use.
5. Specify the name of the database in the **Database** text box.
6. Select the authentication mode and specify the logon credentials, if necessary.
7. Click **Apply** and **OK**.

12 Alerting Options

This chapter provides you with information about configuring the GFI EndPointSecurity alerting options and alerts recipients. Alerting is a crucial part of GFI EndPointSecurity's operation which help you take remedial actions as soon as a threat is detected.

Topics in this chapter

12.1 Configuring alerting options 129

12.2 Configuring the alerts administrator account 131

12.3 Configuring alerts recipients 135

12.4 Configuring groups of alert recipients 135

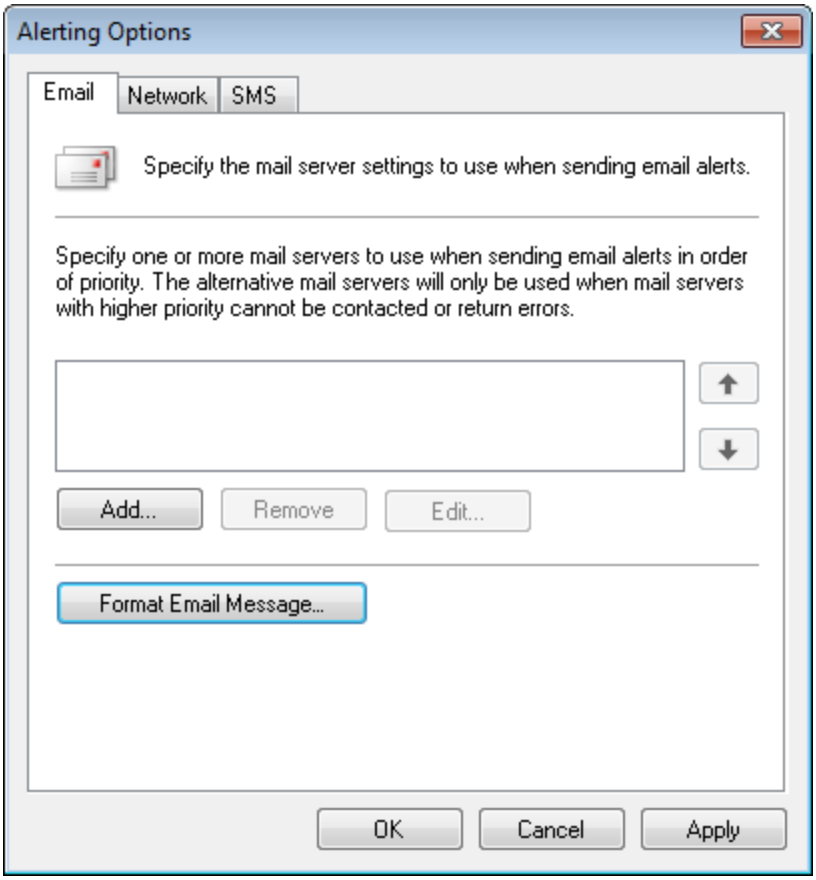
12.1 Configuring alerting options

GFI EndPointSecurity allows you configure the following alerting options:

- The mail server settings, sender details and email message that are used when email alerts
- The network message to use when sending network alerts
- The SMS gateway and SMS message that is used when sending SMS alerts.

To configure alerting options:

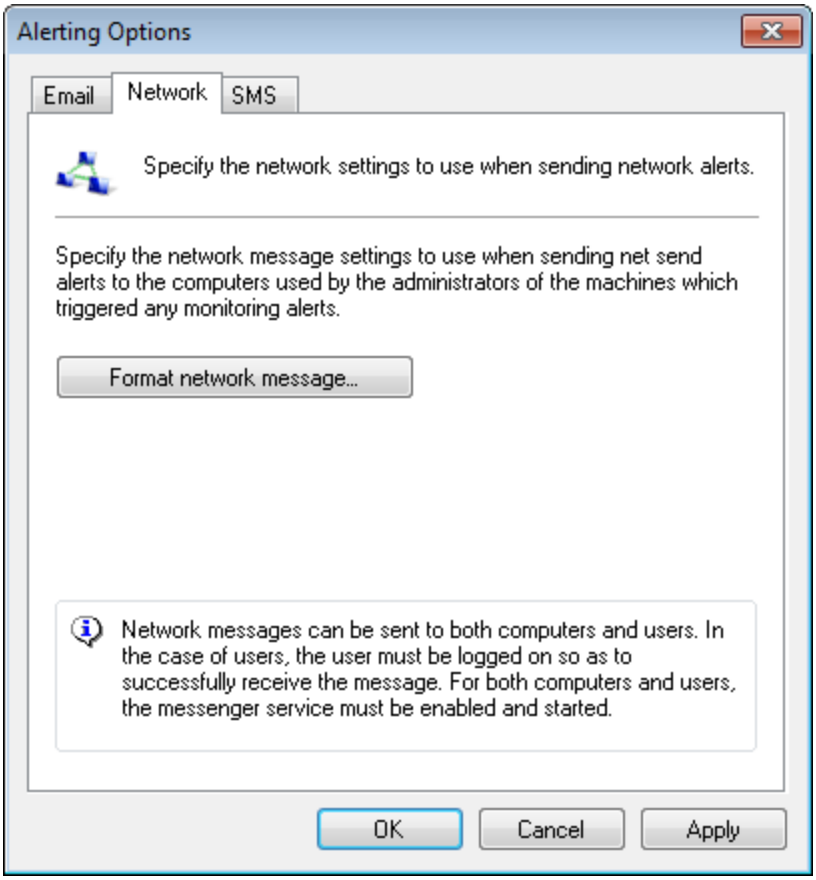
1. Click **Configuration** tab > **Options** sub-tab.
2. From **Configure**, right-click **Alerting Options** node and select **Edit alerting options...**.



Screenshot 103: Alerting Options - Email tab

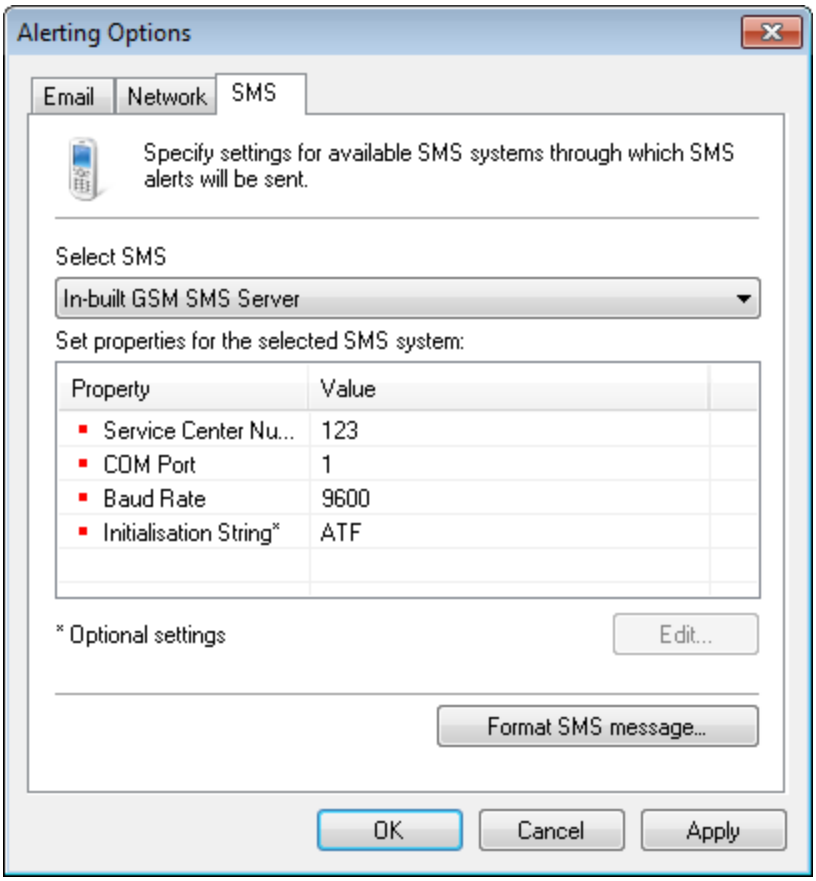
3. From **Email** tab , click **Add...**, to specify your mail server settings. Click **OK** to close the **Mail-server properties** dialog.

4. To edit the email message, click **Format Email Message…**, modify the **Subject** and **Message** fields as required, and click **Save**.



Screenshot 104: Alerting Options - Network tab

5. Click **Network** tab **> Format network message…**, to edit the network message. Click **Save**.



Screenshot 105: Alerting Options - SMS tab

6. Click **SMS** tab and from the **Select SMS** drop-down menu, select the SMS gateway you want to use. Supported SMS systems include:

- In-built GSM SMS Server
- GFI FaxMaker SMS gateway
- Clickatell Email to SMS service gateway
- Generic SMS provides gateway.

7. From the **Set properties for the selected SMS system** area, highlight the property you want to configure and click **Edit**. Repeat this step for each SMS system property you want to modify.

8. Click **Format SMS message…**, to modify the Subject and Message as required. Click **Save**.

9. Click **OK**.

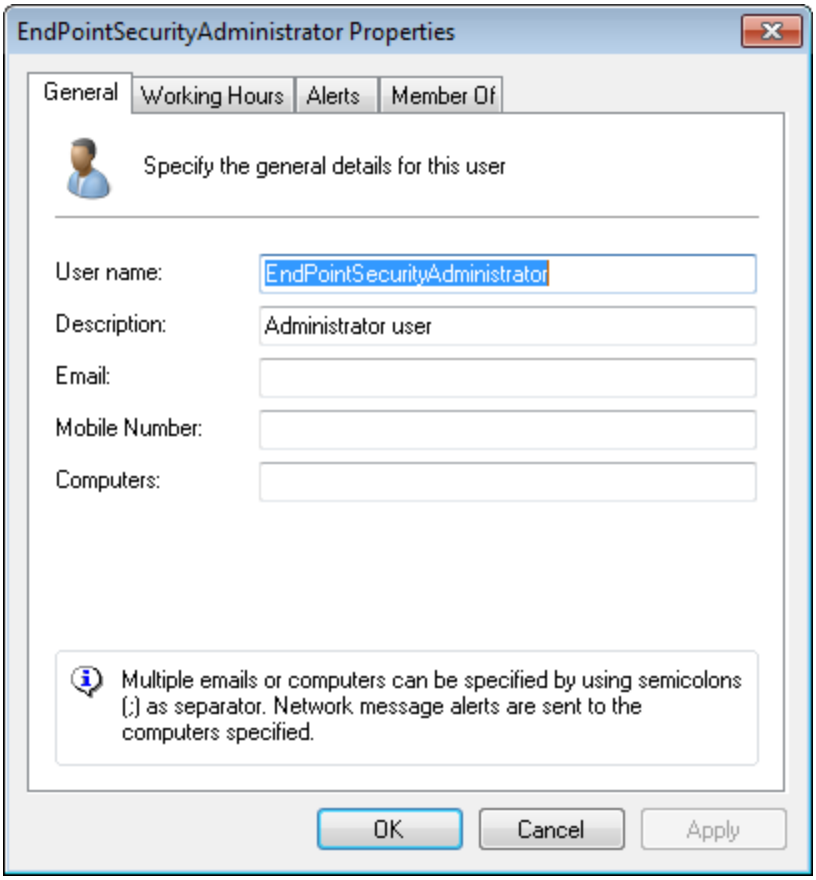
12.2 Configuring the alerts administrator account

GFI EndPointSecurity enables you to configure profile accounts to hold contact details of users intended to receive e-mail alerts, network messages and SMS messages. Upon installation, GFI EndPointSecurityautomatically creates an alerts administrator account. Alert administrators are not Active Directory (AD) users and/or user groups.

By default GFI EndPointSecurity automatically creates the EndPointSecurityAdministrator account (for alerts purposes) upon installation and sets it as a member of the EndPointSecurityAdministrators notification group.

To configure the GFI EndPointSecurityAdministrator account:

1. Click **Configuration** tab > **Options** sub-tab.
2. From **Configure**, click **Alerting Options** > **Users** sub-node.
3. From the right pane, right-click **EndPointSecurityAdministrator** and select **Properties**.

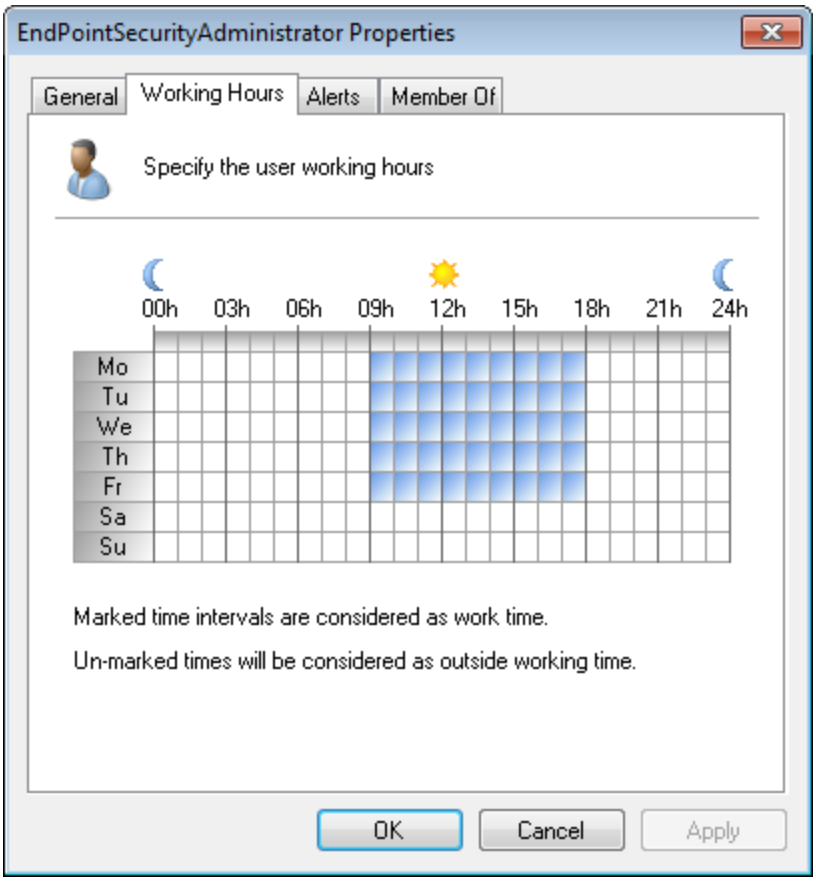


Screenshot 106: EndPointSecurityAdministrator Properties options - General tab

4. From the General tab, key in the following details:

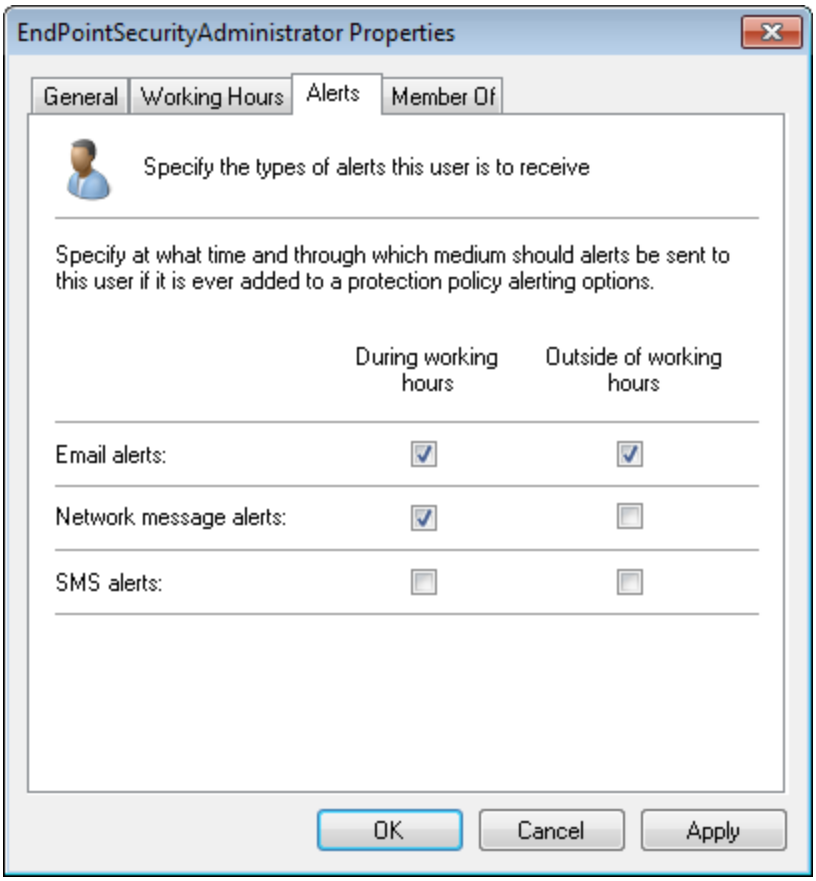
- Account user name
- Account Description
- Email address
- Mobile number
- Computers (network messages are sent to the specified computers)

> **Note**
>
> More than one email address and more than one computer name/IP address can be specified. Separate entries with semicolons ';'.



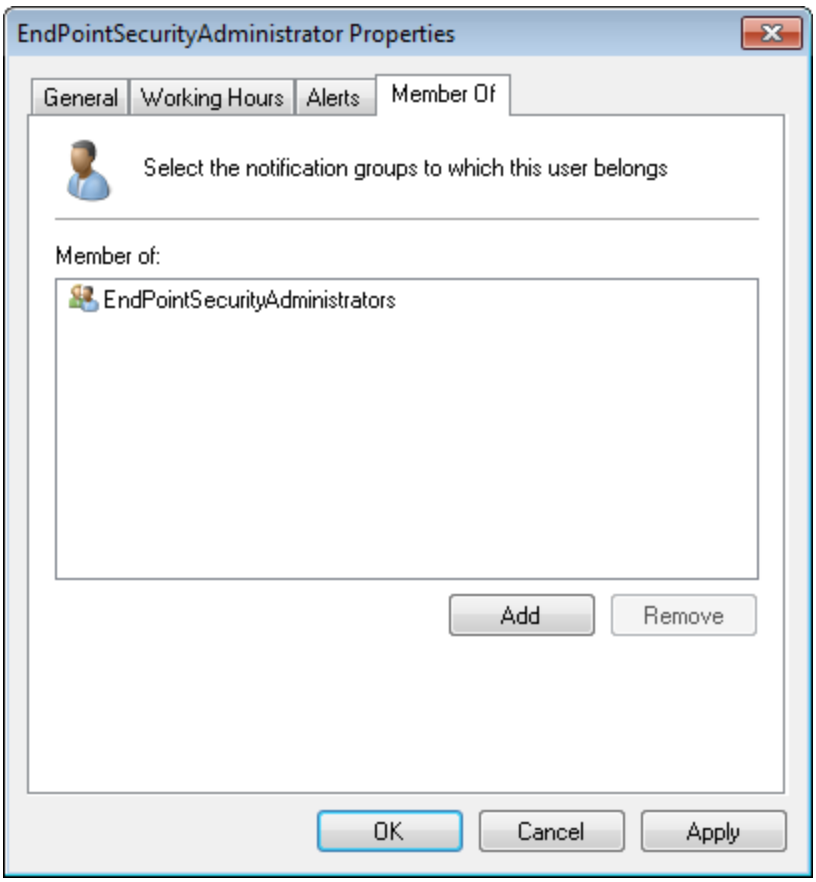
Screenshot 107: EndPointSecurityAdministrator Properties options - Working Hours tab

5. Click **Working Hours** tab and mark the typical working hours of the user. Marked time intervals are considered as working hours.



Screenshot 108: EndPointSecurityAdministrator Properties options - Alerts tab

6. Click **Alerts** tab and select the alerts to be sent and at what time alerts are sent.



Screenshot 109: EndPointSecurityAdministrator Properties options - Member Of tab

7. Click **Member Of** tab and click **Add** to add the user to notification group(s).
8. Click **Apply** and **OK**.

12.3 Configuring alerts recipients

GFI EndPointSecurity enables you to configure other profile accounts (apart from the default GFI EndPointSecurityAdministrator account) to hold the contact details of users intended to receive e-mail alerts, network messages and SMS messages.

Alert recipients are not Active Directory (AD) users and/or user groups, but are profile accounts created by GFI EndPointSecurity to hold the contact details of users intended to alerts.

- Creating alert recipients
- Editing alert recipients properties
- Deleting alert recipients

12.3.1 Creating alert recipients

To create a new alert recipient:

1. Click **Configuration** tab > **Options** sub-tab.
2. From **Configure**, click **Alerting Options > Users** sub-node.
3. From the left pane, click the **Create user…**.
4. For more information about configuring the settings to create a new recipient, refer to Configuring the alerts administrator account.

12.3.2 Editing alert recipient properties

To edit alert recipient's properties:

1. Click **Configuration** tab > **Options** sub-tab.
2. From **Configure**, click **Alerting Options > Users** sub-node.
3. From the right pane, right-click the user you want to edit and select **Properties**.
4. For more information about configuring the settings to edit a recipient, refer to Configuring the alerts administrator account.

12.3.3 Deleting alert recipients

To delete an alert recipient:

1. Click **Configuration** tab > **Options** sub-tab.
2. From **Configure**, click **Alerting Options > Users** sub-node.
3. From the right pane, right-click the user you want to edit and select **Delete**.
4. Click **Yes** to confirm deletion.

12.4 Configuring groups of alert recipients

GFI EndPointSecurity enables you to organize your alert recipients into groups in order to facilitate the management of alert recipients.

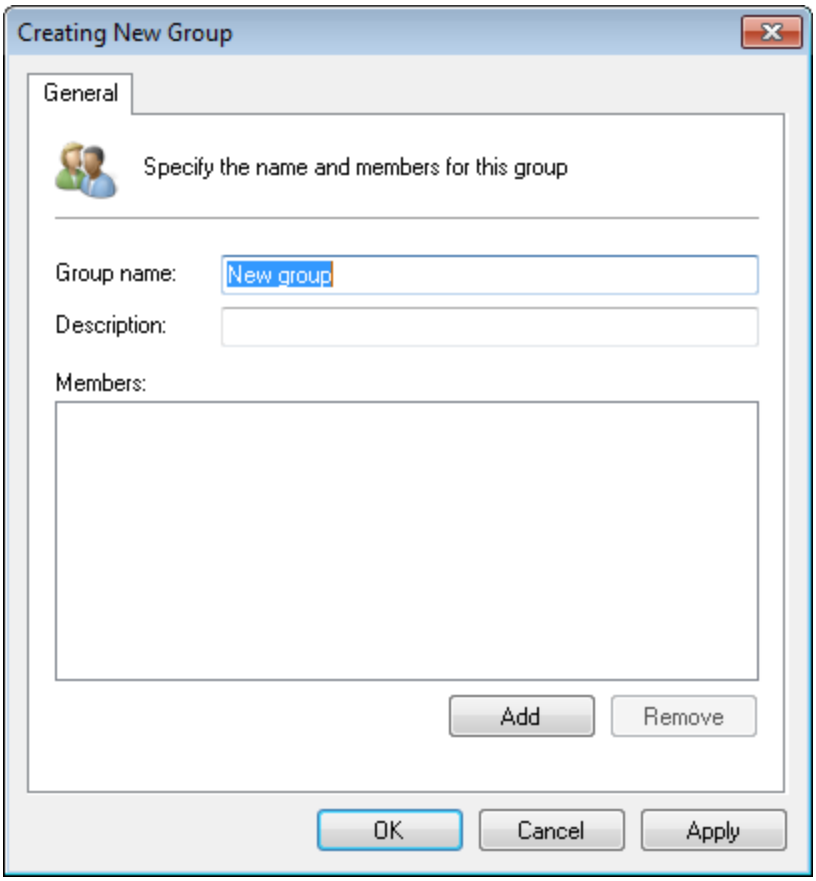
- Creating groups of alert recipients
- Editing group of alert recipients properties

» Deleting groups of alert recipients

12.4.1 Creating groups of alert recipients

To create a new group of alert recipients:

1. Click **Configuration** tab > **Options** sub-tab.
2. Click **Alerting Options** > **Groups** sub-node.
3. From the left pane, click **Create group…**.



Screenshot 110: Creating New Group options

4. From the **Creating New Group** dialog key in the group name and an optional description.
5. Click **Add** to select the user(s) that belong to this notification group, and click **OK**.

12.4.2 Editing group of alert recipients properties

To edit group of alert recipient's properties:

1. Click **Configuration** tab > **Options** sub-tab.
2. Click **Alerting Options** > **Groups** sub-node.
3. From the right pane, right-click the group you want to edit and select **Properties**.
4. For more information on how to edit the settings of groups, refer to Creating groups of alert recipients.

12.4.3 Deleting groups of alert recipients

To delete a group of alert recipients:

1. Click **Configuration** tab **> Options** sub-tab.
2. Click **Alerting Options > Groups** sub-node.
3. From the right pane, right-click the group you want to delete and select **Delete**.
4. Click **Yes** to confirm deletion of the group.

13 Configuring GFI EndPointSecurity

GFI EndPointSecurity enables you to configure the computers you intend to install updates and display user messages on.

Topics in this chapter

13.1 Configuring advanced options 138

13.2 Configuring user messages 140

13.3 Configuring GFI EndPointSecurity updates 141

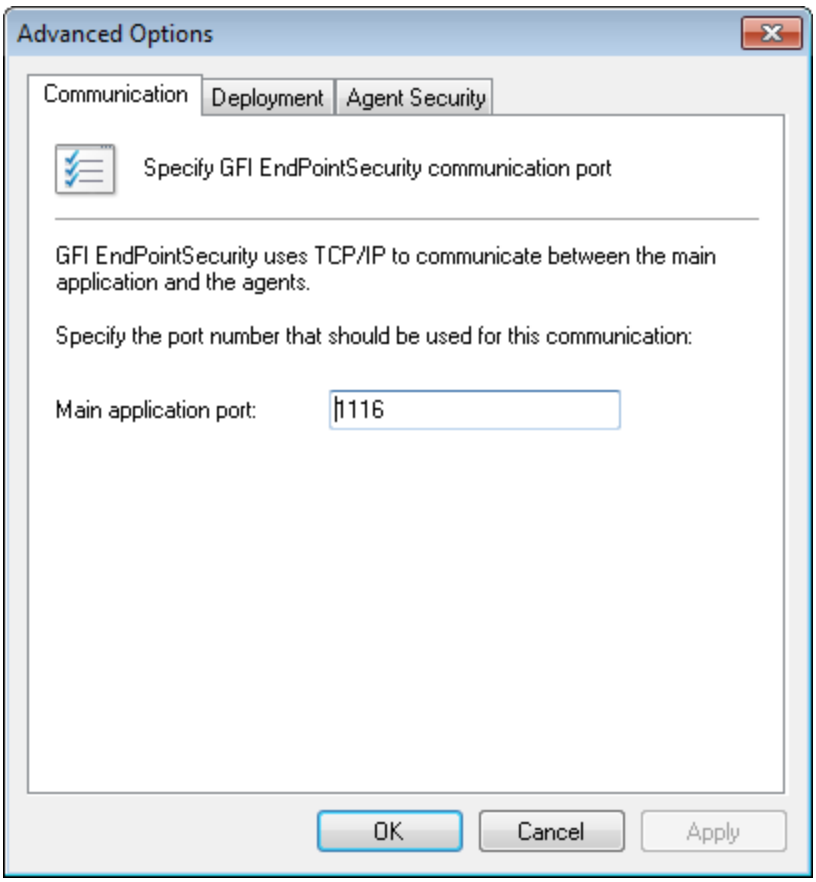
13.1 Configuring advanced options

GFI EndPointSecurity allows you to configure the following Agent advanced options:

- Main communication TCP/IP port
- Deployment options
- Agents control password.

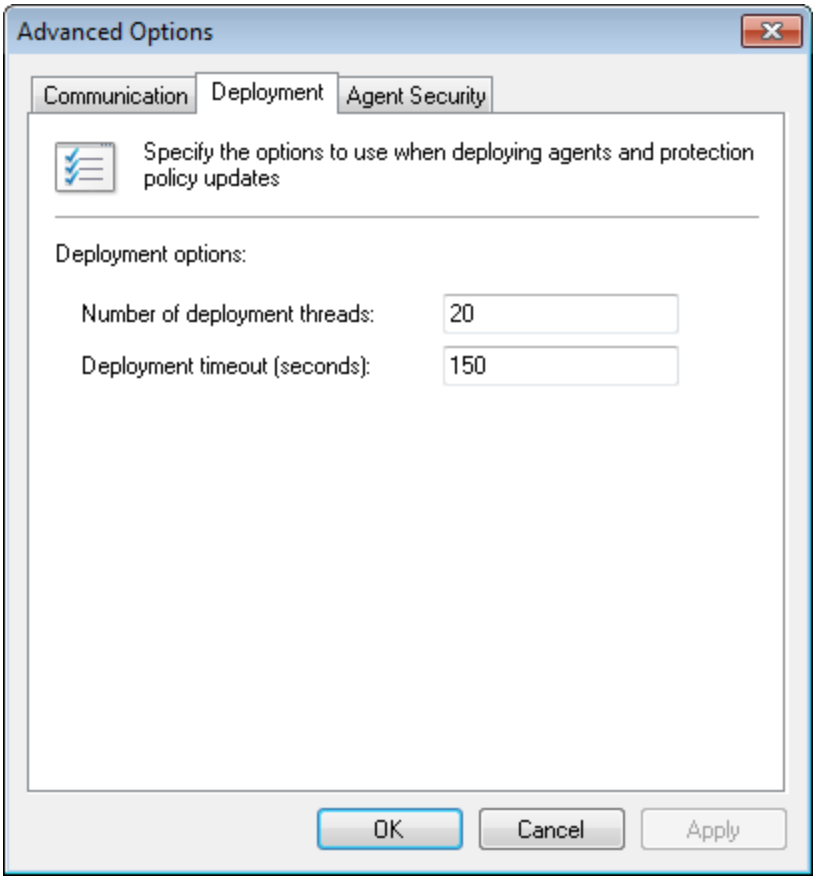
To configure advance options:

1. Click **Configuration** tab > **Options** sub-tab.
2. From **Configure**, right-click **Advanced Options** node and select **Modify advanced options...**.



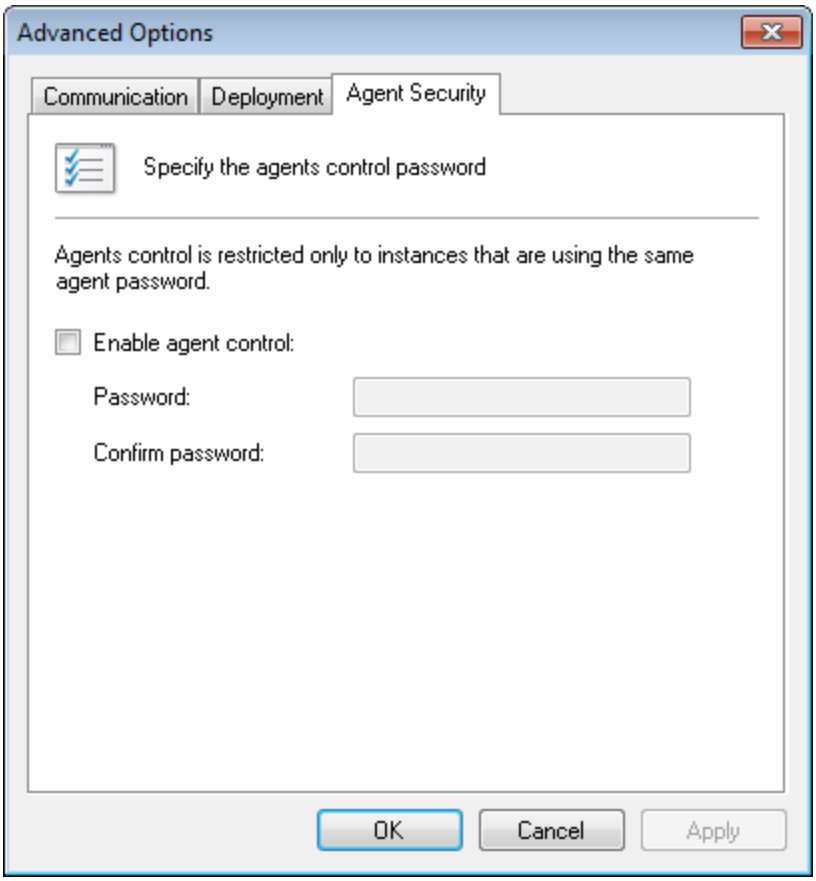
Screenshot 111: Advanced Options - Communication tab

3. From the **Communication** tab, key in the required TCP/IP port number to be used for communication between GFI EndPointSecurity and GFI EndPointSecurity Agents. By default, port **1116** is specified.



Screenshot 112: Advanced Options - Deployment tab

4. Click **Deployment** tab and key in the required **Number of deployment threads** and **Deployment timeout (seconds)** values.



Screenshot 113: Advanced Options - Agent Security tab

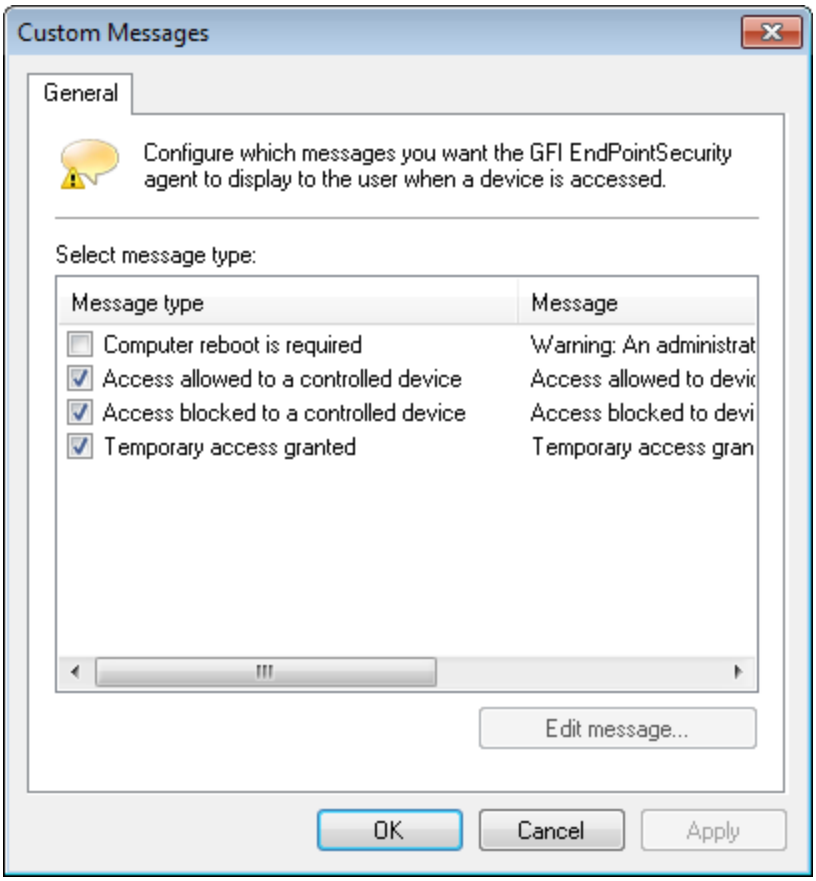
5. Click **Agent Security** tab and select/unselect **Enable agent control**. Use this option to assign particular logon credentials to all GFI EndPointSecurity Agents deployed on your network.
6. Click **Apply** and **OK**.

13.2 Configuring user messages

GFI EndPointSecurity enables you to customize the messages that is displayed by GFI EndPointSecurity Agents on target computers, when devices are accessed.

To customize user messages:

1. Click **Configuration** tab **>** **Options** sub-tab.
2. From Configure, right-click Custom Messages and select Customize user messages.



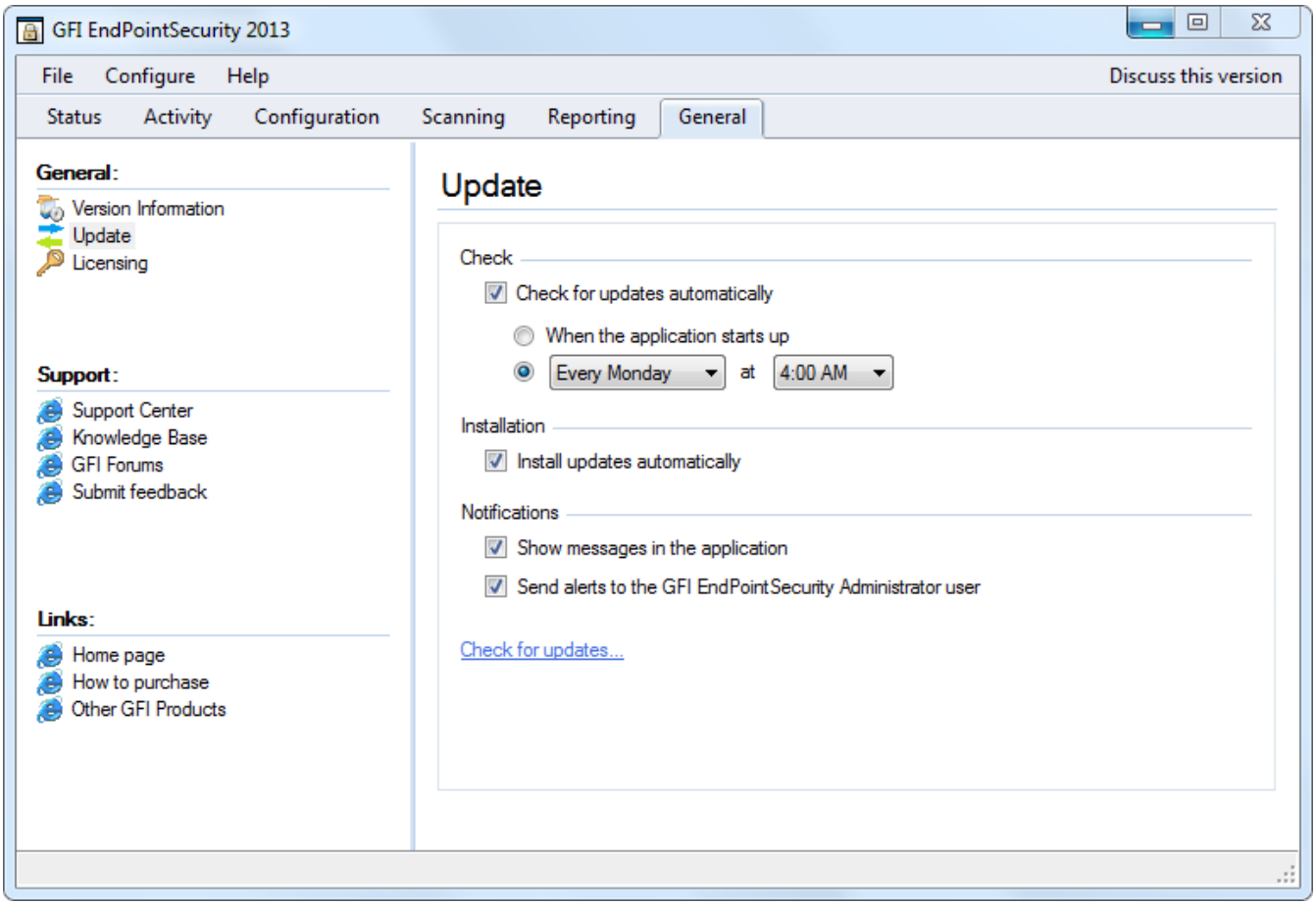
Screenshot 114: Custom Messages dialog options

3. Select/unselect the message types you want to customize.
4. For each message type selected, click **Edit message…**, modify the text as required, and click **Save**. Repeat this step for each message you want to modify.
5. Click **Apply** and **OK**..

13.3 Configuring GFI EndPointSecurity updates

GFI EndPointSecurity can be configured to download and install updates automatically on a schedule or on startup. To configure updates:

1. Click **General** tab.
2. From the left pane, click **Updates**.



Screenshot 115: General tab - Updates

3. From the right pane, configure the options described below:

Table 18: Update options

Option	Description
Check for updates automatically	Connect to the GFI update servers and download product updates automatically. Select When the application starts up, or specify a day and time when to check and download updates.
Install updates automatically	If an update is found, GFI EndPointSecurity will download and install the update automatically.
Show messages in the application	If an update is found and installed, a message is displayed in GFI EndPointSecurity application.
Send alerts to the GFI EndPointSecurityAdministrator user	Once an update is downloaded and installed, an email message is sent to the GFI EndPointSecurity Administrator. For more information, refer to Configuring the alerts administrator account (page 131).
Check for updates	Click the link to instantly run the GFI EndPointSecurity updates engine, download and install any missing updates.

14 Miscellaneous

The miscellaneous chapter gathers all the other information that falls outside the initial configuration of GFI EndPointSecurity.

Topics in this chapter

14.1 Product licensing 143

14.2 Uninstalling GFI EndPointSecurity 143

14.3 Product version information 146

14.1 Product licensing

After installing GFI EndPointSecurity you can enter your license key without re-installing or re-configuring the application.

To enter your license key:

1. Click **General** tab.
2. From the left pane select **Licensing**.

Screenshot 116: Editing license key

3. From the right pane click **Edit...**
4. In the **License Key** text box, key in the license key provided by GFI Software Ltd.
5. Click **OK** to apply the license key.

14.2 Uninstalling GFI EndPointSecurity

GFI EndPointSecurityenables you to easily uninstall both the GFI EndPointSecurity agents and the GFI EndPointSecurity application.

This chapter covers the following topics:

- Uninstalling GFI EndpointSecurity agents
- Uninstalling GFI EndpointSecurity application

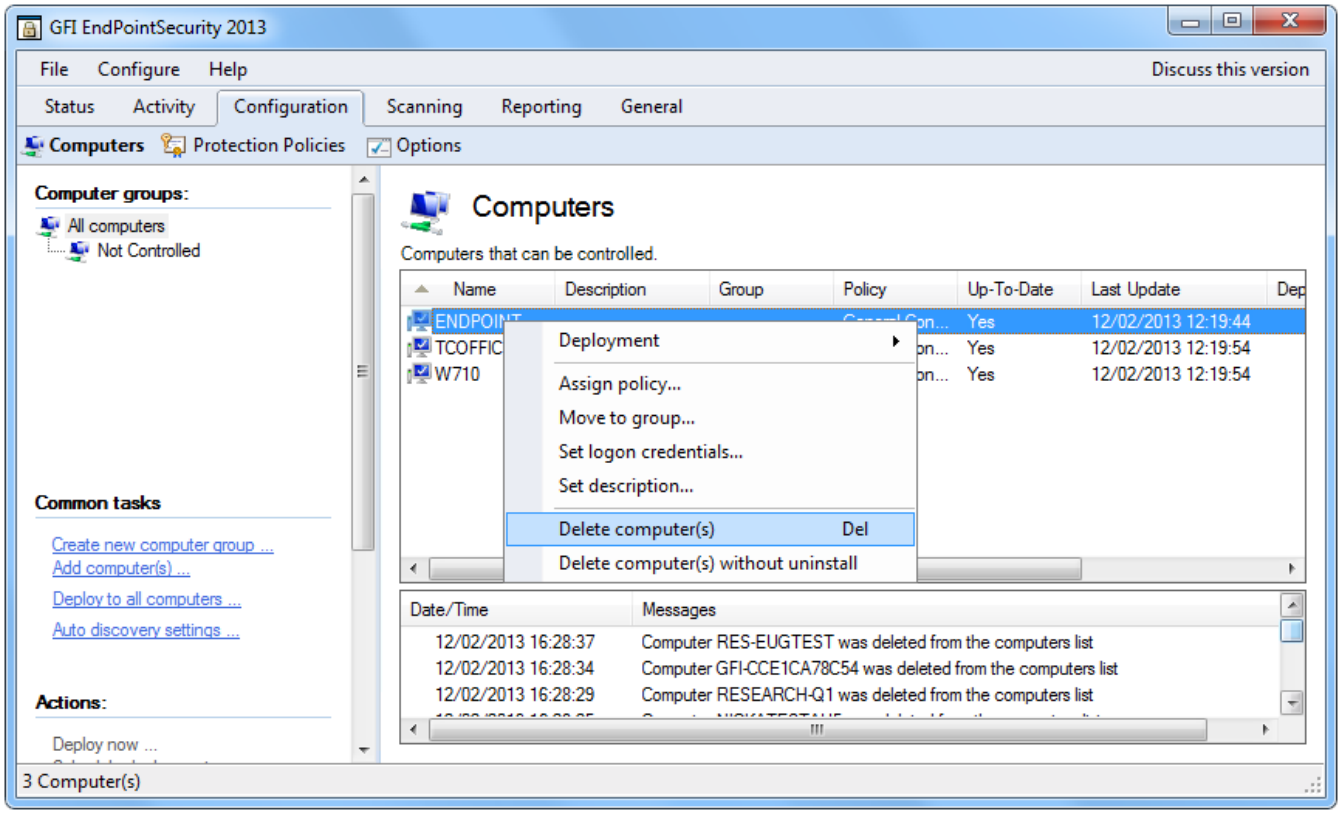
Warning

GFI EndPointSecurity agents are not uninstalled automatically during the un-installation of the GFI EndPointSecurity application. It is best that first you uninstall the GFI EndPointSecurity agents and next the GFI EndPointSecurity application.

14.2.1 Uninstalling GFI EndPointSecurityagents

To uninstall a GFI EndPointSecurityagent:

1. From the GFI EndPointSecurity management console, click **Configuration** tab.
2. Click **Computers** sub-tab.



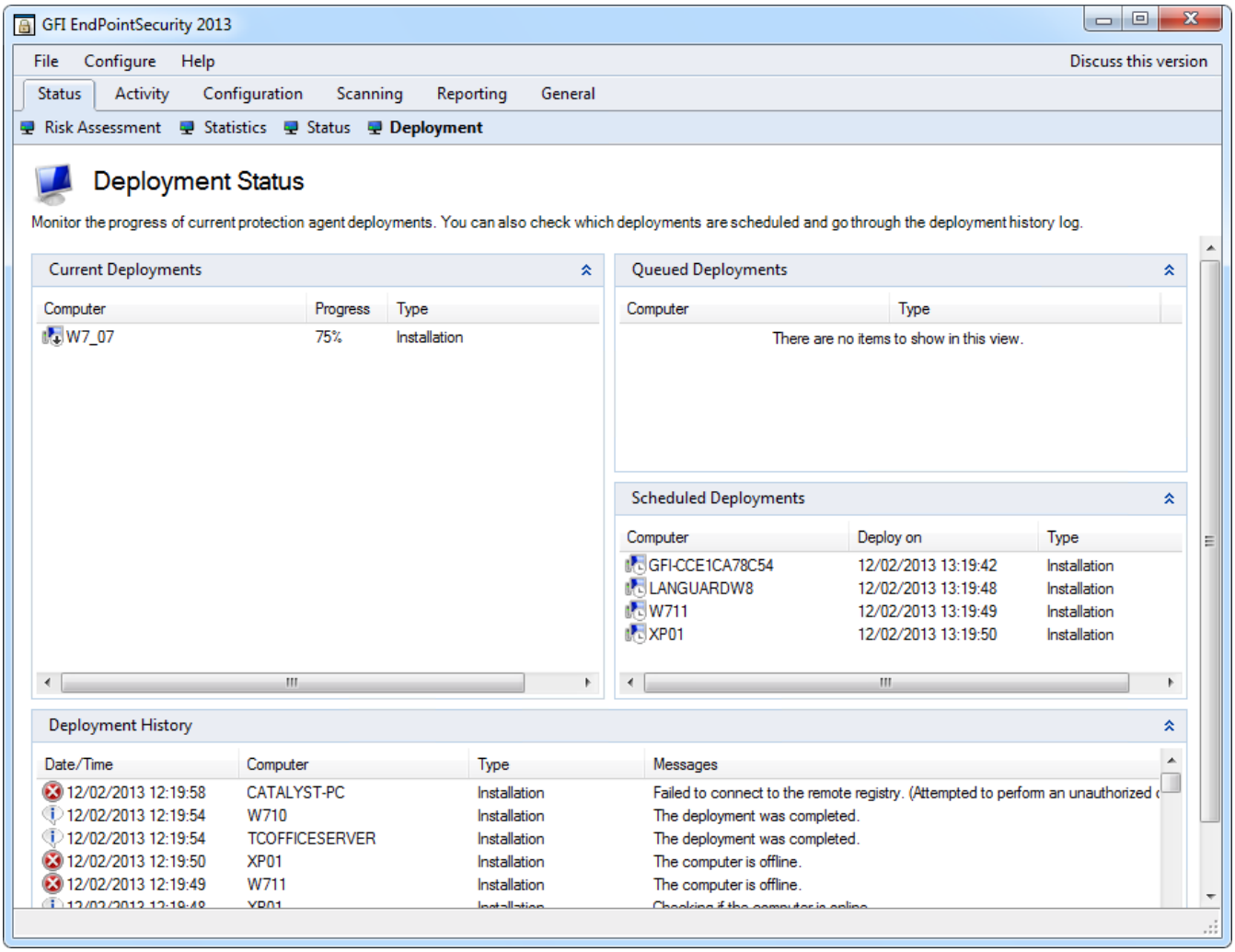
Screenshot 117: Computers sub-tab - delete computer(s)

3. From the right pane, right-click target computer that you would like to uninstall and select:

Deleting Computer(s)	
Deleting computer(s) - **with** uninstallation	GFI EndPointSecurity will deploy protection policy updates and uninstalls Agent.
Deleting computer(s) - **without** uninstallation	GFI EndPointSecurity will deploy protection policy updates and removes the relevant computer entry from the Computers list. However it leaves the agent installed on the target computer. This is useful in the event that the target computer was removed from the network and GFI EndPointSecurityapplication is unable to connect to it to uninstall the agent.

4. Click **Yes** to confirm the deletion of the selected computer from the list.

5. From the right pane, click on the top warning message to deploy the protection policy updates. The view should automatically change to **Status>Deployment**.



Screenshot 118: Deployment sub-tab

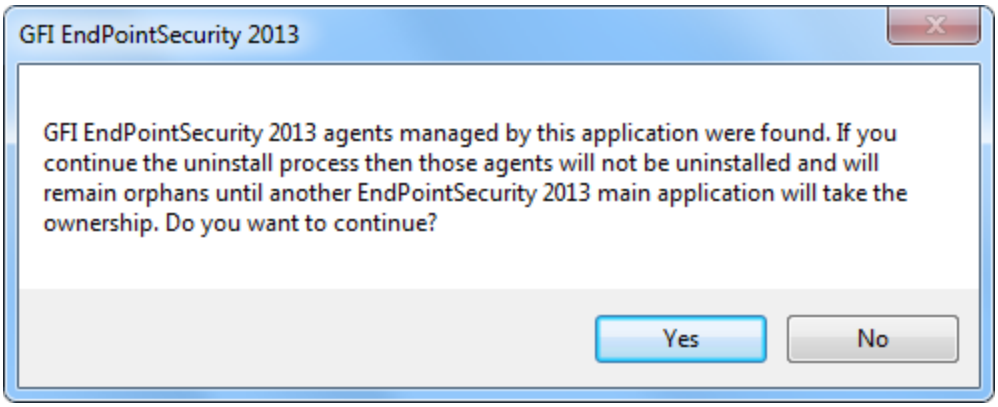
6. From the **Deployment History** area, confirm the successful completion of the un-installation from the target computer.

14.2.2 Uninstalling GFI EndPointSecurityapplication

To uninstall the GFI EndPointSecurity application:

> **Note**
>
> Run the uninstaller as a user with administrative privileges on the computer.

1. From the **Microsoft Windows Control Panel**, select **Add/Remove Programs** or **Programs and Features** option.
2. Select GFI EndPointSecurity.
3. Click **Change** to start the un-installation of GFI EndPointSecurity application.
4. Click **Next** at the Welcome screen to continue un-installation.



Screenshot 119: Uninstallation information message

Note

If any agents are still installed, an information dialog is displayed asking you whether you would like to continue (the agents will remain installed and orphans) or stop the un-installation process. For more information about uninstalling agents, refer to the Uninstalling GFI EndPointSecurity agents section in this chapter.

5. Select **Uninstall without deleting configuration files** or **Complete uninstall** option and click **Next** to continue.
6. Upon completion, click **Finish** to finalize un-installation.

14.3 Product version information

GFI Software Ltd. releases product updates which can be manually or automatically downloaded from the GFI website.

To check if a newer version of GFI EndPointSecurity is available for download:

1. Click **General** tab.
2. From the left pane, select **Version Information**.
3. From the right pane, click **Check for newer version** to manually check if a newer version of GFI EndPointSecurity is available. Alternatively, select **Check for newer version at startup** to automatically check if a newer version of GFI EndPointSecurity is available for download every time the management console is launched.

15 Troubleshooting and Support

This chapter explains how to resolve any issues encountered during installation of GFI EndPointSecurity. The main sources of information available to solve these issues are:

This section and the rest of GFI EndPointSecurity Administrator Guide contains solutions for all possible problems you may encounter. If you are not able to resolve any issue, please contact GFI Support for further assistance.

Common Issues

The table below lists the most common issues which you may encounter during the initial setup and first time use of GFI EndPointSecurity and a possible solution for each:

Table 19: Troubleshooting - Common issues

Issue	Possible Cause	Possible Solution
The computer is offline.	GFI EndPointSecurity management console pings the target computer at deployment to determine whether it is online, and if not this message is displayed.	If a target computer is offline, the deployment of the relevant policy is rescheduled for an hour later. GFI EndPointSecurity keeps trying to deploy that policy every hour, until the target computer is back online. Ensure that the target computer is switched on and connected to the network.
Failed to connect to the remote registry. (error)	GFI EndPointSecurity was not able to extract data from the registry of the target computer.	Ensure that your firewall settings enable communication between the target computers and the GFI EndPointSecurity server. For more information refer to System Requirements.
Failed to gather required information. (error)	GFI EndPointSecurity was not able to extract version related data from the target computer (Operating System version and GFI EndPointSecurity agent version).	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.
Failed to build the required installation files. (error)	GFI EndPointSecurity was not able to add the necessary configuration files within the deployment file (.msi installation file) of the GFI EndPointSecurity agent. This error occurs before the deployment file is copied onto the target computer.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.
Failed to copy the files to the remote computer. (error)	GFI EndPointSecurity was not able to copy the deployment file (.msi installation file) onto the target computer. A possible cause can be that, the administrative share (C$) that GFI EndPointSecurity is using to connect to the target computer, is disabled.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis. For further information about network connectivity and security permissions, refer to: http://kb.gfi.com/articles/SkyNet_Article/KBID003754?retURL=%2Fapex%2FSupportHome&popup=true
Timeout	Agent deployment onto the target computer is either taking too long to complete or else is blocked.	Try to deploy the GFI EndPointSecurity agent again.
Failed to install the deployment service. (error)	GFI EndPointSecurity agent was not able to be installed or uninstalled by the service running on the target computer.	For more details about the cause of the error and a possible solution, refer to the system error message within the parenthesis.

Issue	Possible Cause	Possible Solution
Installation failed.	Installation of the GFI EndPointSecurity agent is complete, but is not marked as installed within the registry.The version and build numbers of the GFI EndPointSecurity agent are not the same as those of the GFI EndPointSecurity management console.	For more details about the cause of the error and a possible solution, refer to the agent installation log files on the target computer at: **%windir%\EndPointSecurity**.
Uninstallation failed.	Uninstallation of GFI EndPointSecurity agent is complete, but is not marked as uninstalled within the registry.	For more details about the cause of the error and a possible solution, refer to the agent installation log files on the target computer at: **%windir%\EndPointSecurity**.
The operation failed due to an unknown exception.	GFI EndPointSecurity has encountered an unexpected error.	Please use the Troubleshooter Wizard to contact the GFI Technical Support team. To open the Troubleshooter Wizard navigate to **Start > Programs > GFI EndPointSecurity 2013 > GFI EndPointSecurity 2013 Troubleshooter**.

Using GFI EndPointSecurity Troubleshooter

To use the troubleshooting tool provided by GFI EndPointSecurity:

1. Click **Start > Programs > GFI EndPointSecurity2013 > GFI EndPointSecurity2013 Troubleshooter**.
2. Click **Next** at the wizard welcome screen.

Screenshot 120: Specifying contact and purchase details

3. Key in your contact details so that our support team would be able to contact you for further analysis information. Click **Next**.

Screenshot 121: Specifying issue details and other relevant information to recreate the problem

4. Specify the error you are getting and other information that would help our support team recreate this issue. Click **Next**.

Screenshot 122: Gathering machine information

5. The troubleshooter scans your system to get hardware information. You can manually add more information in the space provided or click **Next**.

Screenshot 123: Finalizing the Troubleshooter wizard

6. At this stage, the troubleshooter creates a package with the information gathered from the previous steps. Next, send this package to our support team so they can analyze and troubleshoot your problem. Click the buttons described below for sending options:

- **Open Containing Folder** - Opens the folder containing the troubleshooter package so that you can send the package manually via email
- **Go to GFI Support** - Opens the support page of GFI website.

7. Click **Finish**.

GFI SkyNet

GFI maintains a comprehensive knowledge base repository, which includes answers to the most common problems. GFI SkyNet always has the most up-to-date listing of technical support questions and patches. In case that the information in this guide does not solve your problems, next refer to GFI SkyNet by visiting: http://kb.gfi.com/.

Web Forum

User to user technical support is available via the GFI web forum. Access the web forum by visiting: http://forums.gfi.com/.

Request technical support

If none of the resources listed above enable you to solve your issues, contact the GFI Technical Support team by filling in an online support request form or by phone.

- **Online**: Fill out the support request form and follow the instructions on this page closely to submit your support request on: http://support.gfi.com/supportrequestform.asp
- **Phone**: To obtain the correct technical support phone number for your region visit: http://www.gfi.com/company/contact.htm

> **NOTE**
>
> Before contacting Technical Support, have your Customer ID available. Your Customer ID is the online account number that is assigned to you when first registering your license keys in the GFI Customer Area at: http://customers.gfi.com.

We will answer your query within 24 hours or less, depending on your time zone.

Documentation

If this manual does not satisfy your expectations, or if you think that this documentation can be improved in any way, let us know via email on: documentation@gfi.com.

16 Glossary

A

Access permissions

A set of permissions (access, read and write) that are assigned to users and groups per device category, connectivity port or a specific device.

Active Directory

A technology that provides a variety of network services, including LDAP-like directory services.

Alert recipient

A GFI EndPointSecurity profile account to hold the contact details of users intended to receive e-mail alerts, network messages and SMS messages.

Alerts

A set of notifications (e-mail alerts, network messages or SMS messages) that are sent to alert recipients when particular events are generated.

Alerts administrator account

An alert recipient account that is automatically created by GFI EndPointSecurity upon installation.

Automatic discovery

A GFI EndPointSecurity feature to search and discover computers that were newly connected to the network at configured scheduled times.

B

BitLocker To Go

A Microsoft Windows 7 feature to protect and encrypt data on removable devices.

C

Connectivity port

An interface between computers and devices.

Create Protection Policy wizard

A wizard to guide you in the creation and configuration of new protection policies. Configuration settings include the selection of device categories and ports to be controlled and whether to block or allow all access to them. This wizard also allows the configuration of file-type based filters, encryption permissions as well as logging and alerting options.

D

Database backend

A database used by GFI EndPointSecurity to keep an audit trail of all events generated by GFI EndPointSecurity agents deployed on target computers.

Deployment error messages

Errors that can be encountered upon deployment of GFI EndPointSecurity agents from the GFI EndPointSecurity management console.

Device blacklist

A list of specific devices whose usage is blocked when accessed from all the target computers covered by the protection policy.

Device category

A group of peripherals organized in a category.

Device scan

A GFI EndPointSecurity feature to search for all devices that are or have been connected to the scanned target computers.

Device whitelist

A list of specific devices whose usage is allowed when accessed from all the target computers covered by the protection policy.

Digest report

A summary report giving an account of the activity statistics as detected by GFI End-PointSecurity.

E

Event logging

A feature to record events related to attempts made to access devices and connection ports on target computers and service operations.

F

File-type filters

A set of restrictions that are assigned to users and groups per file-type. Filtering is based on file extension checks and real file type signature checks.

G

GFI EndPointSecurity agent

A client-side service responsible for the implementation/enforcement of the protection policies on the target computer(s).

GFI EndPointSecurity application

A server-side security application that aids in maintaining data integrity by preventing unauthorized access and transfer of content to and from devices and connection ports.

GFI EndPointSecurity management console

The user interface of the GFI EndPointSecurity server-side application.

GFI EndPointSecurity Temporary Access tool

A tool which is available on the target computers. It is used by the user to generate a request code and later to enter the unlock code in order to activate the temporary access once it is granted by the administrator. Upon activation, the user will have access to devices and connection ports (when such access is normally blocked) on his protected target computer for the specified duration and time window.

Global permissions

A Create Protection Policy wizard step that prompts the user to either block or else to allow access to all devices falling in a category or which are connected to a port of the target computers covered by the protection policy.

GPO

See Group Policy Objects.

Group Policy Objects

An Active Directory centralized management and configuration system that controls what users can and cannot do on a computer network.

H

Human Interface Devices

A specification that is part of the universal serial bus (USB) standard for a class of peripheral devices. These devices, such as a mice, keyboards, and joysticks, enable users to input data or to interact directly with the computer.

M

MSI file

A file generated by GFI EndPointSecurity for later deployment using GPO or other deployment options. It can be generated for any protection policy and contains all the relevant configured security settings, including installation settings for unprotected target computers.

P

Power user

A power users is automatically given full access to devices connected to any target computer covered by the protection policy.

Protection policy

A set of device access and connectivity port permissions that can be configured to suit your company's device access security policies.

Q

Quick Start wizard

A wizard to guide you in the configuration of GFI EndPointSecurity with custom settings. It is launched upon the initial launch of GFI EndPointSecurity management console and is intended for first time use.

S

Security encryption

A set of restrictions configured to either block or else to allow users/groups to access specific file-types stored on devices that are encrypted with BitLocker To Go. These restrictions are applied when the encrypted devices are connected to the target computers covered by the protection policy.

T

Target computer

A computer that is protected by a GFI EndPointSecurity protection policy.

Temporary access

A period of time during which users are allowed to access devices and connection ports (when such access is normally blocked) on protected target computers, for a specified duration and time window.

U

User message

A message that is displayed by GFI EndPointSecurity agents on target computers, when devices are accessed.

17 Index

A

access permissions 30, 33, 35, 49, 60, 63, 65, 68

Active Directory 12, 14, 34, 36, 50, 54, 59-60, 63, 65, 68, 70, 81, 96, 123, 131, 135

alert recipients 35, 96, 135

alerts 14, 16, 35, 51, 96, 118, 123, 129, 131, 135, 142

alerts administrator account 35, 131, 135

automatic discovery 40

B

BitLocker To Go 13, 88

C

Common Issues 147

connectivity port 51, 108, 117

D

database backend 14, 22, 27, 37, 110, 126, 128

device blacklist 35, 70, 105

device category 31, 61, 68, 115

Device Scan 103

device whitelist 35, 74, 105

digest report 123

E

event logging 36, 51, 94

F

file-type filters 77, 81

G

GFI EndPointSecurity

agent

application

management console

Temporary Access tool

version 11-14, 16-19, 21-23, 25, 27, 29-30, 33-35, 37-39, 42, 45, 51, 54-55, 57-60, 63, 65, 68, 70, 74, 77, 81, 83, 86, 88, 94, 96, 99-100, 104, 106, 109, 113, 116, 118, 120, 123, 126, 129, 131, 135, 138, 140-141, 143, 145-147

Glossary 150

H

Human Interface Devices 18, 47, 58

L

licensing 20, 25, 28, 143

M

msi file 54

P

power users 15, 26, 30, 33, 35, 59, 70

protection policy 13-14, 17, 23, 29-30, 34, 36, 38-39, 42, 45, 51-54, 57, 59-61, 63, 65, 68, 70-71, 74, 79, 81, 83, 86, 88, 94, 96, 99-100, 104, 119, 122, 144

Q

Quick Start wizard 25, 29, 126

S

security encryption 88

supported connectivity ports 58

supported device categories 57, 100

T

target computer 17, 22, 38, 51-53, 100, 104, 117, 144, 147

Technical Support 148

temporary access 13-14, 17, 35, 77

Troubleshooter wizard 148

Troubleshooting 147

U

user messages 35, 138, 140

V

versions 11

W

Web Forum 149

wizard

Create Protection Policy wizard

Quick Start wizard

Troubleshooter wizard 25, 47, 148

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104 Cary, NC 27513, USA

Telephone: +1 (888) 243-4329

Fax: +1 (919) 379-3402

ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK

Telephone: +44 (0) 870 770 5370

Fax: +44 (0) 870 770 5377

sales@gfi.com

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta

Telephone: +356 2205 2000

Fax: +356 2138 2419

sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia

Telephone: +61 8 8273 3000

Fax: +61 8 8273 3099

sales@gfiap.com

GFI®